نظرية التشفير والتعمية (الأساسيات)

الجزء الأول

تأليف

د. ر. هانكرسون | د. غ. هوفمان

د. أ. لينورد | ك. ك. ليندنر

ك. ت. فيلبس | ك. أ. روجر

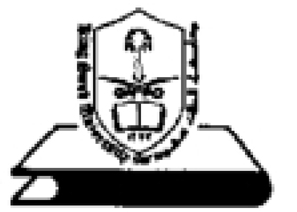
ج. ر. وول

ترجمة

د. معروف عبدالرحمن سمحان | د. فوزي بن أحمد الذكير

قسم الرياضيات - كلية العلوم

جامعة الملك سعود




النشر العلمي والمطابع - جامعة الملك سعود

ص.ب ٦٨٩٥٣ - الرياض ١١٥٣٧ - المملكة العربية السعودية

هذه ترجمة عربية مصرح بها من مركز الترجمة بالجامعة لكتاب:

Coding Theory and Cryptography: The Essentials
By: D. R. Hankerson, *et al*.

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

د. ر. هانكرسون

نظرية التشفير والتعمية: الأساسيات./ د. ر. هانكرسون؛ معروف عبدالرحمن سمحان؛ فوزي بن أحمد الذكير.- الرياض، ١٤٣٥هـ

٢مج.

٣٧١ص؛ ١٧×٢٤سم

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٢-٢١٨-٥٠٧-٦٠٣-٩٧٨ (ج١)

١- الشيفرة ٢- الاختصارات ٣- أمن المعلومات أ. سمحان، معروف عبدالرحمن (مترجم) ب. الذكير، فوزي بن أحمد (مترجم) ج. العنوان

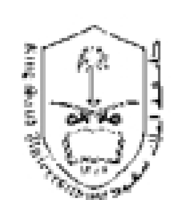
ديوي ٦٥٢,٨ ١٤٣٥/٩٨

رقم الإيداع: ٩٨/ ١٤٣٥

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٢-٢١٨-٥٠٧-٦٠٣-٩٧٨ (ج١)

حكمت هذا الكتاب لجنة متخصصة، وقد وافق المجلس العلمي على نشره في اجتماعه العشرين للعام الدراسي ١٤٣٣هـ/ ١٤٣٤هـ المعقود بتاريخ ١٦/ ٧/ ١٤٣٤هـ الموافق ٢٦/ ٥/ ٢٠١٣م.



النشر العلمي والمطابع ١٤٣٥هـ

مقدمة المترجمين

وقع اختيارنا على ترجمة هذا الكتاب لعدة أسباب أهمّها أن هذا الكتاب يجمع بين موضوعي نظرية التشفير ونظرية التعمية وهما الموضوعان اللّذان نقوم بتدريسهما في مقرر تطبيقات الجبر لطلاب قسم الرياضيات ، ولذا فهو يخدم الهدف الذي نسعى إليه وهو توفير مادة علمية باللغة العربية لهذين الموضوعين لتكون في متناول الطالب. ومما يميز هذا الكتاب هو شرح مادة الرياضيات اللازمة لفهم المواضيع في المكان المناسب وبدون تعمق حيث يتطرق فقط إلى المفاهيم التي يحتاج إليها دون الخوض في براهين رياضية صعبة ، وهذه الميزة تجعل هذا الكتاب مناسباً لطلبة الهندسة والحاسب الآلي بالإضافة إلى طلاب الرياضيات.

أثناء ترجمتنا لهذا الكتاب قمنا بتصحيح بعض الأخطاء المطبعية التي تمكنا من اكتشافها والتي لا يكاد يخلو منها أي كتاب. قمنا أيضاً بوضع بعض التفاصيل للمادة العلمية وأضفنا بعض البراهين التي نعتقد ضرورة وجودها وقد تم ذلك دون الإخلال بتسلسل المادة العلمية.

اعتمدنا في ترجمة المصطلحات العلمية على قاموس العلوم الرياضية الذي شارك المترجمان في إعداده والصادر عن منشورات جامعة الملك سعود وهو مبني على

المعجمين الصادرين عن مكتب تنسيق التعريب بالرباط ومعجم الرياضيات الصادر عن مؤسسة الكويت للتقدم العلمي، واجتهدنا بترجمة المصطلحات التي لم ترد في أي من هذه المعاجم الثلاثة.

ونود أن نشكر مركز الترجمة بجامعة الملك سعود على موافقته على ترجمة هذا الكتاب الذي نأمل أن يكون إضافة مفيدة إلى المكتبة العربية. واللّه من وراء القصد.

المترجمان

إهداء المؤلفين

إلى زوجاتنا الحبيبات

سندي وجيل وجين وآن وجانيت وسو

إلى أولادنا

نويل وأيان وتيم وكيرت وجيمي وأندرو وميخان وكاترينا وريبركا

وإلى آبائنا وأمهاتنا

إيلين وريتشارد، ڤالي وجيل، مارجوري ولويس، ماري وتشارلز،

إيثل وريتشارد، أيريس وأيان، بيولاه ووالتر.

شكر وتقدير
Acknowledgments

نقدم شُكرنا العميق لألفريد مينيزس على اقتراحاته المفصّلة ومراجعاته العديدة للفصول من العاشر إلى الثاني عشر. كان من الممكن أن يحتوي هذا الكتاب على أخطاء أكثر وأن يكون سرد المادة أسوأ لولا ارشاداته الجمّة لنا. كما نود أن نقدم شُكرنا لسيلدا كيوسيكسفي على مراجعتها واقتراحاتها وتصحيحها لبعض الأخطاء. أما روزي توربرت فقد ساهمت مساهمة غير عادية بإنجاز أصول الطبعة الأولى من هذا الكتاب.

إن صبرها وشجاعتها على تحمل الأعباء الناتجة عن المراجعات الكثيرة يضعها في مصاف القديسين. كما نقدم شُكرنا وتقديرنا لهيذر كونر على العمل الرائع التي قامت به أثناء التحضير للطبعة الثانية. ونخص بالشكر مصممة الغلاف سندي أوترسون كما نقدر لها عملها معنا في العديد من المشاريع.

المؤلفون

تمهيد
Preface

الهدف من هذا الكتاب المنقّح والمحدّث من الطبعة الأولى هو تدريس نظرية التشفير والتعمية بأسلوب رياضي معقول لطلبة الهندسة وعلوم الحاسب والرياضيات. يختلف هذا الكتاب عن معظم كتب التشفير والتعمية الأخرى بنقطتين مهمتين هما "في الوقت المناسب" وإهمال التعميمات الرياضية غير المهمة.

إن فلسفة "في الوقت المناسب" مبنيّة على تقديم مادة الرياضيات اللازمة عند الحاجة إلى تطبيقها، ولذا، فالكتاب لا يحتوي على ٢٠٠ صفحة من الرياضيات (ليست ضرورة في معظمها) ومن ثم ٢٠٠ صفحة أخرى من التشفير والتعمية. وبهذا فإن شكل الكتاب هو على النحو التالي: رياضيات، تطبيقات، رياضيات، تطبيقات وهكذا. إن تجنب التعميمات الرياضية يعني على سبيل المثال، أنه ليس من الضروري وصف الشفرة الدورية على أنها مثالي رئيس. وبهذا فلقد أهملنا في العموم الخوض في التعميمات الرياضية والمفاهيم التي تستخدم عادة لتدريس المقرّر لطلاب الرياضيات فقط.

استخدم الجزء الأول من هذا الكتاب (الفصول من الأول إلى التاسع) لتدريس نظرية التشفير في فصلين متتاليين في جامعة أوبرن حيث كان المتطلب الوحيد أن يكون

لدى الطالب معلومات بدائية في الجبر الخطي. وبالطبع كلما كانت معلومات الطالب في الجبر الخطي والجبر المجرّد أكثر يكون استيعابه أفضل ومن ثم يحتاج إلى وقت أقصر لتغطية المادة الأوليّة.

يُركّز جزء نظرية التشفير من هذا الكتاب على إنشاء الشفرات الثنائية والشفرات على حقل مميزه 2، كما يُركّز على عمليتي التشفير وفك التشفير (تصويب الأخطاء) لعائلة من الشفرات المهمة. وعائلة الشفرات المختارة ذات أهمية خاصة للمهندسين ومتخصصي علوم الحاسب مثل شفرات ريد وسولومن وشفرات التلاف المستخدمة في اتصالات الفضاء وإلكترونيات المستهلك، ويعكس هذا الخيار المدى الواسع لخوارزميات التشفير وفك التشفير

أما الجزء الثاني من هذا الكتاب (الفصول من العاشر إلى الثاني عشر) فتبلورت فكرته بعد تدريسنا مقرراً بدائياً لفصل واحد في نظرية التعمية لطلاب جامعة أوبرن حيث الطلاب المسجلون في هذا المقرر هم خليط من طلاب مرحلة البكالوريوس وطلاب الدراسات العليا من تخصصات علوم الحاسب، الهندسة، الرياضيات، التربية حيث إن المعرفة الرياضية لبعضهم تقتصر على مقرر بدائي في الجبر أو نظرية الأعداد، ويعتبر ذلك كافياً لتقديم مقرر معقول في علم التعمية. في الحقيقة إن معظم المادة العلمية في هذا المقرر تحتاج فقط إلى النتائج الأساسية للأعداد الصحيحة قياس n (وهذه مقدمة في الفصل الحادي عشر). إن هدفنا الأساسي هو كتابة مقرر مختصر وتام لمقدمة في التعمية الحديثة مع التركيز على طرائق التعمية ذات المفتاح المعلن. في الفصل الثاني عشر قمنا بتغطية المواضيع الرئيسة في بنود قصيرة نسبياً وتركنا بعض الموضوعات للتمارين (تحتوي هذه التمارين على بعض التفاصيل والمراجع).

بوجه عام، نستطيع القول إن اهتمام نظرتي التعمية والتشفير هو نقل المعلومات إلكترونياً، مع مراعاة السرّية في الأولى والموثوقية في الثانية ومع اعترافنا بأن معظم الخطط الدراسية لا يتسع فيها المجال لتخصيص مقررات منفصلة لكل منها فإن هذا الكتاب يتيح تدريس الفصول من الأول إلى الرابع ومن ثم الفصلين الخامس والسادس أو الفصلين السابع والثامن لمقرر واحد في نظرية التشفير. من الممكن أيضاً تدريس الفصول من العاشر إلى الثاني عشر لمقرر في نظرية التعمية. كما أنه من الممكن تدريس الفصول الأول والثاني والثالث والعاشر والثاني عشر مع بعض موضوعات الفصل الحادي عشر لمقرر في التشفير والتعمية.

وأخيراً فالمؤلفون سيكونون ممتنين لأي ملحوظات يقدمها لهم مستخدمو هذا الكتاب على العنوان الإلكتروني: rodgec1@auburn.edu.

الرموز
Symbols

$C^{\perp}$: شفرة ثنوية للشفرة C .

C_{23} : شفرة جولاي.

C_{24} : شفرة جولاي الممتدة.

$GF(2^r)$: حقل جالوا.

$GF\left(2^r\right)[x]$: كثيرات حدود بمعاملات في الحقل $GF(2^r)$.

$RM(r,m)$: شفرة ريد ومولر.

$RS(2^r,\delta)$: شفرة ريد وسولومن.

S : الشفرة المولّدة بالمجموعة S .

المحتويات
Contents

الجزء الثاني: نظرية التعمية

الفصل الأول

مقدمة في نظرية التشفير
Introduction to Coding Theory

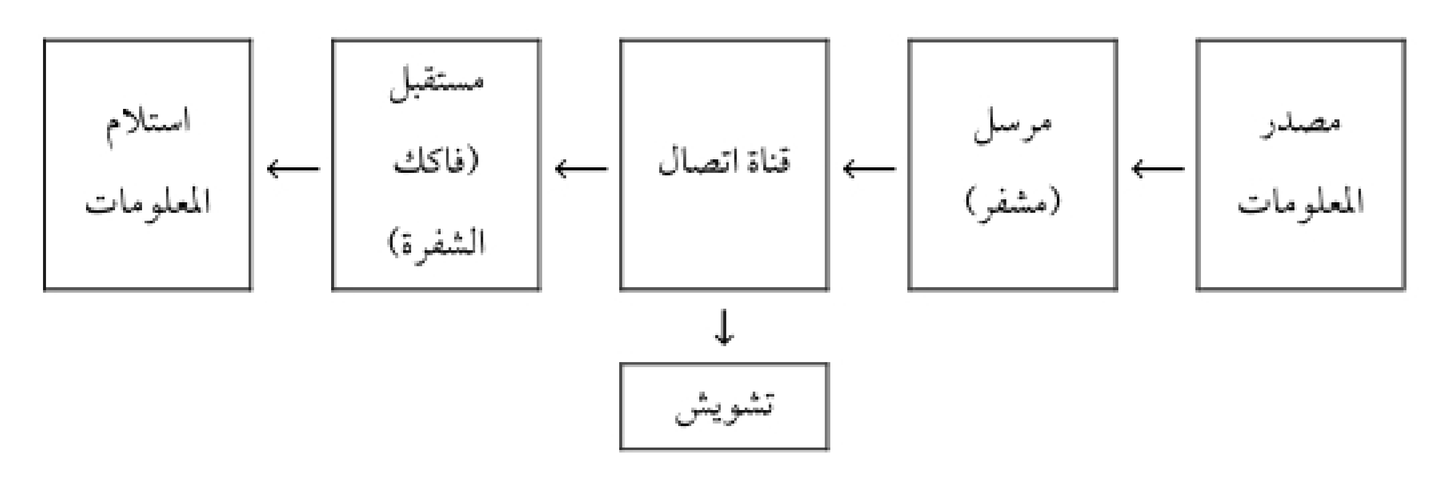
(١,١) مقدمة
Introduction

نظرية التشفير (أو الترميز) هي دراسة طرائق النقل الفعّال والدقيق للمعلومات من مكان إلى آخر. تم تطوير هذه النظرية لتغطية تطبيقات متنوعة مثل خفض التشويش في التسجيل على الأقراص المدمجة إلى الحد الأدنى، عملية إرسال المعلومات المالية عبر خطوط الهاتف، عملية نقل البيانات من جهاز حاسب لآخر أو من الذاكرة إلى المعالج المركزي، إرسال المعلومات من مصادر بعيدة مثل الأقمار الصناعية الجويّة أو أقمار الاتصالات الصناعية أو مركبة فضائية تستخدم لإرسال صور من كوكبي المشتري وزحل إلى الكرة الأرضية.

يُسمى الوسط المادي الذي يتم نقل المعلومات بواسطته، قناة اتصال أو **قناة (Channel)**. خطوط الهاتف والغلاف الجوي مثالان على القناة. يُسمى الإزعاج غير المرغوب فيه الذي ينتج عنه اختلاف بين المعلومات المرسلة والمعلومات المستقبلة، **التشويش (Noise)**. إن مسببات التشويش عديدة مثل: كُلَف الشمس (بقع داكنة تبدو بين فترة وأخرى على سطح الشمس)، البرق، انحناءات في شريط مغناطيسي، أمطار،

تداخلات في خطوط الهاتف، إزعاج عشوائي في المذياع، أخطاء مطبعية، ضعف في السمع، عدم وضوح في الكلام وأمثلة أخرى كثيرة.

ينصب اهتمام نظرية التشفير على مسألة اكتشاف وتصويب أخطاء الارسال الناتجة عن التشويش في قناة الاتصال. المخطط التالي يقدم لنا فكرة عامة عن ماهية نظام إرسال معلومات.



إن أهم جزء من هذا المخطط بالنسبة لنا هو التشويش ؛ لأنه بغياب التشويش تكون نظرية التشفير عديمة الفائدة.

في التطبيق العملي يكون بمقدورنا تقليل التشويش عند اختيارنا لقناة اتصال مناسبة لنقل المعلومات واستخدام مرشحات تشويش مختلفة لمقاومة بعض أنماط التدخلات التي يمكن أن تقابلنا وهذا من مهام المهندسين. وبمجرد الاتفاق على اختيار أفضل نظام ميكانيكي لحل هذه المسائل نستطيع التركيز على إنشاء **المشفّر وفاكك التشفير (Encoder & Decoder)** وتكون رغبتنا في هذا الإنشاء تحقيق ما يلي :

(١) سرعة تشفير المعلومات.

(٢) سهولة نقل الرسائل المشفّرة.

(٣) سرعة فك تشفير الرسائل المستقبلة.

(٤) تصويب الأخطاء الناتجة عن التشويش.

(٥) القدرة على نقل معلومات بحد أقصى لكل وحدة زمن.

الخاصية (٤) هي الهدف الأساس لنظرية التشفير، ولكن هذه الخاصية ليست متناغمة مع الخاصية الخامسة ومن الممكن أن لا تكون متناغمة مع باقي الخواص. ولذا لإيجاد حل فلا بد من المقايضة بين الأهداف الخمسة.

نستخدم في اتصالاتنا اليومية كلمات سواء أكانت شفهية أم مكتوبة وهذه الكلمات مكوّنة من حروف هجائية محدودة. ولتبادل معلومات نقوم بتشفيرها إلى متتالية من الكلمات ومن ثم نتكلم هذه الكلمات أو نكتبها وبعد ذلك نرسلها عبر قناة اتصال وهي في العادة الفضاء من الفم إلى الأُذن أو من القلم إلى الورقة ومن ثم إلى العين. أما التشويش فقد يتسبب من عدم وضوح في الكلام أو ضعف في السمع أو خطأ نحوي أو موسيقى عالية أو تداخل في الكلام أو خطأ في الإملاء أو خطأ في القراءة أو خطأ مطبعي. وأخيراً يكون فك التشفير هو قراءتنا (أو سماعنا) وفهمنا للرسالة المستقبلة. ونتيجة لذلك نكون قد أنشأنا أدوات لتصويب الأخطاء دون أن نتعمد ذلك. فلنفرض أننا استقبلنا الرسالة "Apt natural. I have a gub" وهي تحذير مكتوب لعملية سطو مأخوذ من فيلم "احصل على النقود واهرب" **لودي آلن** (**Woody Allen**). وبما أن كلمات الهجائية الإنجليزية ذات الطول الواحد والتي لها معنى هي كلمات محدودة فيكون من الواضح أن "gub" ليست كلمة ذات معنى. وبهذا فإننا نفترض أن الكلمة المرسلة قريبة من الكلمة "gub". ومن ثم فهي على الأرجح "gut" أو "gun" أو "tub" وليست "firetruck" أو "rat". ومن فحوى الرسالة فقط نرجح أن الكلمة هي "gun". أما الكلمة "Apt" فهي كلمة ذات معنى (تعني ملائم) ولكنها لا تتلاءم مع فحوى الرسالة ومن ثم نرجح وقوع خطأ في الإرسال ونُصوّبها على أنها "act". وإذا كنا متعلمين ومتقنين لقواعد اللغة فإننا نقوم بتصويب "natural" لتكون "naturally" على الرغم من أن الاحتمال الأكبر لهذا الخطأ هو المصدر وليس التشويش في قناة الاتصال. سنتعامل فقط مع الأخطاء من النوع الأول. أي سنختار الكلمة التي على الأرجح قد تم إرسالها.

إن الطريقة التقليدية المتبعة لتجنب الأخطاء هي تذييل الرسالة بمعلومات زائدة حيث عديد من الجهات تضيف رقماً إضافياً إلى الأعداد المستخدمة للتعريف بالمنتج وتستخدم هذه الإضافات لاختبار صحة البيانات أو أرقام الحسابات وهذه هي الطريقة الشائعة الاستخدام في عملية التشفير في الأعمال اليومية. الأفكار التي سنناقشها في هذا الكتاب هي أفكار مشابهة ولكنها أكثر تطوراً.

(١,٢) فرضيات أساسية
Basic Assumptions

نقدم الآن بعض التعاريف والفرضيات الأساسية التي سنستخدمها في هذا الكتاب.

في عديد من الحالات تُستخدم المتتاليات الثنائية (حدودها مكوّنة من الرقمين 0 و 1) لنقل المعلومات المزمع إرسالها. ولهذا يُسمى كل من الرقمين 0 أو 1 **إحداثياً (Digit)**. **الكلمة (Word)** هي متتالية من الإحداثيات. **طول الكلمة (Length of Word)** هو عدد الإحداثيات المكوّنة للكلمة. فمثلاً 0110101 كلمة طولها سبعة. وتتم عملية نقل الكلمة بإرسال الإحداثيات واحدة بعد الأخرى عبر **قناة ثنائية (Binary Channel)**. وقناة ثنائية هنا تعني أن الإحداثيين المستخدمين هنا هما 0 و 1 فقط. كل إحداثي من إحداثيات الكلمة يتم إرساله ميكانيكياً أو كهربائياً أو مغناطيسياً أو بأي وسيلة أخرى، وأياً كانت الوسيلة فذلك يكون على شكل نبضات يسهل تمييز بعضها عن بعض (أي أن نبضة الإحداثي 0 مختلفة عن نبضة الإحداثي 1).

تعرّف **الشفرة الثنائية (Binary Code)** على أنها مجموعة C من الكلمات. فمثلاً، الشفرة المكوّنة من جميع الكلمات ذات الطول 2 هي:

$$C = \{00\,,10\,,01\,,11\}$$

الشفرة القالبية (Block Code) هي شفرة أطوال جميع كلماتها متساوية ويُسمى هذا الطول الموحّد، **طول الشفرة (Length of the Code)**. سندرس في هذا الكتاب

الشفرات القالبية فقط ولهذا فعند قولنا شفرة نعني دائماً أنها شفرة قالبية ثنائية. تُسمى الكلمات المكوّنة لشفرة معطاة C ، **كلمات شفرة (Code Words)**. سنرمز لعدد كلمات شفرة C بالرمز $|C|$.

تمارين

(١,٢,١) اكتب جميع الكلمات ذات الطول 3 وجميع الكلمات ذات الطول 4 وجميع الكلمات ذات الطول 5.

(١,٢,٢) جد صيغة لعدد الكلمات من الطول n

(١,٢,٣) لتكن C الشفرة المكوّنة من جميع الكلمات ذوات الطول 6 بحيث تحتوي كل كلمة على عدد زوجي من الإحداثيات 1. اكتب كلمات الشفرة C.

نحتاج أيضاً لوضع بعض الفرضيات الأساسية على قناة الاتصال، هذه الفرضيات ستحدد الشكل الذي تقوم عليه نظرية التشفير.

الفرضية الأولى هي افتراض أن كلمة الشفرة من الطول n مكوّنة من إحداثيات 0 وإحداثيات 1 ويتم استقبالها ككلمة طولها n مكوّنة من إحداثيات 0 وإحداثيات 1 والتي لا تكون بالضرورة الكلمة المرسلة نفسها.

الفرضية الثانية هي سهولة تحديد بداية كل من الكلمات المرسلة. على سبيل المثال، عند استخدامنا لكلمات شفرة من الطول 3 واستقبالنا للمتتالية 011011001 فتكون الكلمات المرسلة هي 011 ,011 ,001 على التوالي (تتم قراءة المتتالية من اليسار إلى اليمين)، وهذا يعني استحالة أن تكون القناة قد أرسلت المتتالية 01101100 إلى المستقبل؛ لأن عدد الإحداثيات لا يقسم على 3.

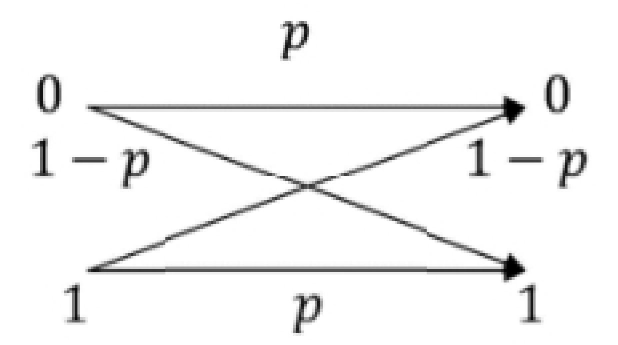
والفرضية الأخيرة هي أن التشويش متناثر عشوائياً وليس على شكل كتل تُدعى **اندفاعات (Bursts)**. إن هذا يعني أن احتمال تأثر إحداثي أثناء الإرسال يساوي احتمال تأثر أي إحداثي آخر ولا يتأثر بالأخطاء التي قد تكون حصلت لإحداثيات

مجاورة. هذه الفرضية ليست واقعية للعديد من أنماط التشويش مثل البرق أو خدوش الأقراص المدمجة. سنتعامل لاحقاً مع مثل هذه الأنماط من التشويش.

في حالة القناة المثالية (عدم وجود تشويش)، يكون الإحداثي المرسل 0 أو 1 هو الإحداثي المستقبل. وبهذا إذا كانت جميع القنوات مثالية فلا حاجة لنا إلى نظرية التشفير. ولكن لحسن الحظ (أو ربما لسوء الحظ) جميع القنوات غير مثالية ومشوّشة ولكن تشويش بعضها أقل من تشويش بعضها الآخر. أي أن بعضها أكثر موثوقية من بعضها الآخر.

نقول إن القناة الثنائية **متماثلة (Symmetric)** إذا كانت الدقّة في ارسال 0 و 1 متساوية. أي أن احتمال استقبال الإحداثي الصحيح لا يعتمد على أي من الإحداثيين 0 أو 1 قد يكون أُرسل. وتعرّف **موثوقية (Reliability)** قناة ثنائية متماثلة (اختصاراً BSC) على أنها عدد حقيقي p حيث $0 \leq p \leq 1$ و p هو احتمال أن يكون الإحداثي المرسل هو الإحداثي المستقبل (أي احتمال عدم حدوث خطأ في الإحداثي).

ولهذا إذا كان p هو احتمال أن يكون الإحداثي المستقبل هو نفس الإحداثي المرسل فإن $1-p$ هو احتمال أن يكون الإحداثي المستقبل ليس هو الإحداثي المرسل. المخطط التالي يبين عمل القناة BSC:



في معظم الأحيان يكون من الصعب حساب الموثوقية p بصورة دقيقة لقناة معطاة ولكن ذلك ليس له تأثير مباشر على نظرية التشفير.

نقول إن قناة ما أكثر موثوقية من قناة أخرى إذا كانت موثوقيتها أعلى من موثوقية القناة الأخرى. لاحظ أن الحالة $p = 1$ لا تهمنا ؛ لأنه لا يوجد أخطاء في الإرسال ومن ثم فإن القناة مثالية. كما أن القنوات التي يكون فيها $p = 0$ ليست بذات أهمية. لاحظ أيضاً إمكانية تحويل قناة تحقق $0 < p \leq \frac{1}{2}$ إلى قناة تحقق $\frac{1}{2} \leq p < 1$. ولهذا فإننا سنفترض دائماً أن قنوات BSC المستخدمة هي قنوات باحتمال p حيث $\frac{1}{2} < p < 1$. (الحالة التي يكون فيها $p = \frac{1}{2}$ هي فحوى التمرين (١,٢,٦)).

تمارين

(**١,٢,٤**) بيّن لماذا تكون القناة ليست بذات أهمية عندما $p = 0$.

(**١,٢,٥**) بيّن كيفية تحويل قناة تحقق $0 < p \leq \frac{1}{2}$ إلى قناة تحقق $\frac{1}{2} \leq p < 1$.

(**١,٢,٦**) ماذا يمكن القول عن قناة تحقق $p = \frac{1}{2}$ ؟

(١,٣) تصويب واكتشاف أنماط الأخطاء

Correcting & Detecting Error Patterns

ندرس الآن امكانية تصويب واكتشاف الأخطاء. ففي هذا البند نعالج مفهومي تصويب واكتشاف الأخطاء حدسياً ونؤجل المعالجة الرياضية لبنود لاحقة.

لنفرض أننا استقبلنا كلمة ووجدنا أنها ليست كلمة شفرة. عندئذ، يكون من الواضح أن خطأ ما قد حصل أثناء عملية الإرسال وبهذا نكون قد اكتشفنا خطأً (أو عدة أخطاء). أما إذا كانت الكلمة المستقبلة هي كلمة شفرة فتكون إمكانية عدم حصول أخطاء في الإرسال واردة ومن ثم لا نستطيع اكتشاف أي خطأ. أما مفهوم تصويب خطأ فيحتاج إلى المزيد من التمحيص. وكما بيّنا في المقدمة عند ميلنا لتصويب الكلمة "gub" إلى "gun" وليس إلى "rat" فحدسُنا يقودنا إلى اقتراح تصويب كلمة مرسلة إلى كلمة شفرة بحيث تكون الأقرب إلى الكلمة المرسلة (أي تغيير أقل عدد ممكن من

الإحداثيات). سنبيّن في بند لاحق أن احتمال أن تكون كلمة الشفرة هذه هي الكلمة التي تم إرسالها لا يقل عن احتمال إرسال أي كلمة شفرة أخرى. سنوضح ذلك بدراسة بعض الأمثلة للشفرات مع ملاحظة افتراضنا عدم سقوط أو إضافة أي إحداثي أثناء الإرسال. فمثلاً ، نفترض استحالة فك تشفير "gub" إلى "firetruck".

مثال (١,٣,١)

لنفرض أن $C_1 = \{00, 01, 10, 11\}$. عندئذ، جميع الكلمات المستقبلة هي كلمات شفرة ومن ثم فإن C_1 لا تستطيع اكتشاف أي خطأ. كما أن C_1 لا تصوّب أي أخطاء؛ لأن جميع الكلمات المستقبلة هي كلمات شفرة ومن ثم لا تتطلب أي تغيير فيها. ▲

مثال (١,٣,٢)

إذا كرّرنا كلاً من كلمات الشفرة C_1 ثلاث مرات نحصل على الشفرة:

$$C_2 = \{000000, 010101, 101010, 111111\}$$

هذا مثال على ما يُسمى **شفرة مكرّرة (Repetition Code)**. لنفرض أننا استقبلنا الكلمة 110101. بما أن هذه ليست كلمة شفرة، فلذا لا بد من وقوع خطأ واحد على الأقل أثناء عملية الإرسال. وبملاحظة أنه يمكن الحصول على كلمة الشفرة 010101 بتغيير إحداثي واحد فقط ولكن يتطلب الحصول على كلمات الشفرة الأخرى إلى تغيير أكثر من إحداثي واحد، فنرجح أن تكون كلمة الشفرة 010101 هي المرسلة وبهذا نُصوّب 110101 إلى 010101. (تُسمى كلمة الشفرة التي نحصل عليها من كلمة w بتغيير أقل عدد من الإحداثيات، كلمة **الشفرة الأقرب (Closest Codeword)** وسنقوم لاحقاً بتعريفها بدقة أكثر). في الحقيقة، إذا تم إرسال أي كلمة شفرة $c \epsilon C_2$ ووقع خطأ واحد أثناء الإرسال فإن كلمة الشفرة الوحيدة الأقرب إلى الكلمة المستقبلة هي c نفسها ومن ثم فإن الشفرة C_2 تصوّب خطأ واحد فقط. ▲

مثال (١,٣,٣)

إذا أضفنا إحداثياً ثالثاً لكل كلمة من كلمات الشفرة C_1 بحيث يصبح عدد الإحداثيات 1 في كل من كلمات الشفرة زوجياً نحصل على الشفرة:

$$C_3 = \{000\,, 011\,, 101\,, 110\}$$

يسمى الإحداثي المضاف **إحداثي اختبار النوعية (Parity–Check Digit)**. إذا استقبلنا الكلمة 010 وهي ليست كلمة شفرة يكون بإمكاننا اكتشاف وقوع خطأ في الإرسال ويمكن الحصول على كل من كلمات الشفرة 110 و 000 و 11 بتغيير إحداثي واحد في الكلمة المستقبلة. في البنود القادمة سنفرق بين تعاملنا مع الكلمات المستقبلة الأقرب إلى كلمة شفرة وحيدة (ومن ثم تكون كلمة الشفرة الوحيدة المرجح إرسالها) كما هو الحال في المثال (١,٣,٢) وبين الكلمات المستقبلة الأقرب إلى عديد من كلمات الشفرة كما هو الحال في هذا المثال. سنكتفي في هذه المرحلة بملاحظة أنه من الأنسب تصويب 010 لتكون أي من 110 ، 000 ، 011 ولكن ليس 101. ▲

تمارين

(**١,٣,٤**) لتكن C شفرة جميع الكلمات ذات الطول 3. إذا استقبلنا الكلمة 001 فبيّن أي كلمة شفرة تكون قد أُرسلت على الأرجح.

(**١,٣,٥**) أضف إحداثي اختبار النوعية لكلمات الشفرة المقدمة في التمرين (**١,٣,٤**) ومن ثم استخدم الشفرة C الناتجة عن ذلك للإجابة عن الأسئلة التالية:

(أ) إذا استقبلنا الكلمة 1101 فهل بإمكاننا اكتشاف خطأ ؟

(ب) إذا استقبلنا الكلمة 1101 فما هي كلمة الشفرة التي تكون على الأرجح قد أُرسلت ؟

(ج) هل توجد كلمة طولها 4 وليست كلمة شفرة بحيث تكون الأقرب إلى كلمة شفرة وحيدة ؟

(١,٣,٦) كرّر كلاً من كلمات الشفرة C المبينة في التمرين **(١,٣,٤)** ثلاث مرات لتحصل على شفرة تكرار من الطول 9. جد كلمة الشفرة الأقرب إلى كل من الكلمات المستقبلة :

(أ) 001000001 (ب) 011001011

(ج) 101000101 (د) 100000010

(١,٣,٧) جد أكبر عدد من كلمات الشفرة ذات الطول 4 المحتواة في شفرة تستطيع اكتشاف خطأ واحد أياً كان هذا الخطأ.

(١,٣,٨) كرّر التمرين **(١,٣,٧)** عندما يكون $n = 5$ و $n = 6$ وبعد ذلك لأي n.

(١,٤) معدل المعلومات
Information Rate

يتضح لنا من البند السابق أن إضافة إحداثيات لكلمات الشفرة يزيد من قدرة الشفرة على تصويب واكتشاف الأخطاء. ومن الواضح أيضاً أنه كلما ازداد طول كلمة الشفرة ازداد الزمن اللازم لإرسال الرسالة. **معدل المعلومات (Information Rate)** للشفرة هو عدد مصمم لقياس الجزء من كل كلمة شفرة الذي يتضمن الرسالة. يعرّف معدل معلومات الشفرة C ذات الطول n (للشفرات الثنائية) على أنه :

$$\frac{1}{n} log_2|C|$$

وبما أن $1 \leq |C| \leq 2^n$ فمن الواضح أن معدل المعلومات يقع بين 0 و 1. فهو يساوي 1 إذا كانت كل كلمة هي كلمة شفرة ويساوي 0 إذا كان $|C| = 1$.

على سبيل المثال، معدل معلومات الشفرات C_1 ، C_2 ، C_3 المقدمة في البند السابق هو 1، $\frac{1}{3}$ ، $\frac{2}{3}$ على التوالي. كل من معدلات المعلومات هذه تتلاءم مع الشفرة ذات الصلة. لاحظ أن أول إحداثيين من الستة إحداثيات لكل من كلمات الشفرة C_2

هما اللذان يتضمنان الرسالة وأن الإحداثيين الأول والثاني من الإحداثيات الثلاثة لكل من كلمات الشفرة C_3 هما اللذان يتضمنان الرسالة.

تمرين

(**١,٤,١**) احسب معدل المعلومات لكل من الشفرات المقدمة في التمارين (**١,٣,٤**)، (**١,٣,٥**)، (**١,٣,٦**).

(١,٥) تأثير تصويب واكتشاف الأخطاء

The Effect of Error Correction & Detection

لفهم مدى التأثير الناتج عن إضافة إحداثي اختبار النوعية إلى شفرة على اكتشاف وتصويب الأخطاء، ندرس المثال التالي:

نفرض أن جميع الكلمات ذات الطول 11 وعددها $2^{11} = 2048$ هي كلمات شفرة. عندئذ، لا يمكننا اكتشاف أي خطأ. لنفرض أن موثوقية القناة هي $p = 1 - 10^{-8}$ ولنفرض أن معدل إرسال الإحداثيات هو 10^7 إحداثي في الثانية. حينئذ، يكون احتمال وجود خطأ في الكلمة المرسلة هو $11p^{10}(1-p) \approx 11/10^8$. وبهذا نرى أن عدد الكلمات المرسلة والتي تحتوي على خطأ لا يتم اكتشافه هو $\frac{11}{10^8} \times \frac{10^7}{11} = 0.1$ كلمة في الثانية الواحدة أو كلمة واحدة خطأ كل 10 ثوانٍ أو 6 كلمات خطأ كل دقيقة أو 360 كلمة خطأ كل ساعة أو 8640 كلمة خطأ كل يوم !

لنفرض الآن أننا أضفنا إحداثي اختبار النوعية لكل كلمة من كلمات الشفرة بحيث يكون عدد الإحداثيات 1 في كل منها زوجياً. عندئذ، يمكن اكتشاف أي خطأ واحد ومن ثم لكي تحتوي الكلمة المرسلة على أخطاء لا يمكن اكتشافها فيجب أن يكون عدد الأخطاء على الأقل 2. ولذا فاحتمال وقوع خطأين على الأقل يساوي:

$$\binom{12}{2} P^{10}(1-p)^2 = 66(1-10^{-8})^{10} \times 10^{-16} \approx 66 \times 10^{-16}$$

ويكون عدد الكلمات المرسلة والتي تحتوي أخطاء لا يتم اكتشافها هو $\frac{66}{10^{16}} \times \frac{10^7}{12} \approx 5.5 \times 10^{-9}$ كلمة في الثانية أو كلمة واحدة كل 2000 يوم !

مما سبق نرى أن إضافة إحداثي واحد إلى كل من كلمات الشفرة ليصبح الطول يساوي 12 عوضاً عن 11 يُبيّن لنا سهولة اكتشاف الأخطاء عند وقوعها. ولتصويب هذه الأخطاء نطلب إعادة إرسال الرسالة وهذا يعني توقف عملية الإرسال حتى نحصل على تأكيد أو تخزين الرسائل لفترة مؤقتة لحين طلب إعادة الإرسال وتكون التكاليف باهظة في كلتا الحالتين سواء على صعيد الزمن اللازم أو سعة التخزين. كما أنه من الممكن أن تكون عملية إعادة الإرسال غير عملية كما في المراكب الفضائية أو استخدام الأقراص المدمجة. ولتخفيض الثمن الباهظ الناتج عن زيادة طول كلمات الشفرة فيكون من المناسب إضافة بعض قدرات تصويب الأخطاء للشفرة. ولكن إضافة مثل هذه القدرات قد ينتج عنه صعوبة في التشفير وفك التشفير ولكنه يساعد على تخفيض التكاليف في الزمن وسعة التخزين المبينة للشفرة المقدمة في بداية هذا البند.

إحدى الخطط المساعدة على تصويب الأخطاء هي إنشاء شفرة تكرار حيث يتم إرسال كل من كلمات الشفرة ثلاث مرات متتالية. فإذا وقع خطأ واحد على الأكثر في كل كلمة شفرة من الطول 33 فنكون قد ضمنا صحة إرسالين على الأقل من الإرسالات الثلاثة. وبما أن مقارنة ثلاث كلمات من الطول 11 أمر سهل فإن الثمن الوحيد الذي يدفع لتصويب خطأ هو تخفيض معدل المعلومات من 1 إلى $\frac{1}{3}$.

سنبين لاحقاً إمكانية إضافة 4 إحداثيات فقط لكل من كلمات الشفرة ذات الطول 11 لجعلها قادرة على تصويب خطأ واحد ومن ثم يكون معدل المعلومات هو $\frac{11}{15}$ وهو أفضل بكثير من $\frac{1}{3}$ إذا تجاهلنا الإعاقة الناتجة عن ذلك في عملية التشفير وفك التشفير.

نخلص إلى القول إن مهمتنا هي تصميم شفرات بمعدل معلومات معقول وثمن معقول لعملتي التشفير وفك التشفير مع القدرة على تصويب واكتشاف بعض الأخطاء لتلافي الحاجة إلى إعادة الإرسال.

(١,٦) إيجاد الاحتمالية القصوى لكلمة الشفرة المرسلة
Finding the Most Likely Codeword Transmitted

لنفرض أن لدينا فكرة عامة عن عملية الإرسال وأننا على معرفة بكلمة الشفرة v المرسلة والكلمة w المستقبلة. لكل v و w نفرض أن $\varphi_p(v,w)$ هو احتمال استقبال الكلمة w إذا كانت v هي كلمة الشفرة المرسلة عبر قناة BSC بموثوقية p. وبما أننا افترضنا أن توزيع التشويش هو توزيع عشوائي نرى أن كل إرسال إحداثي هو **حدث (Event)** مُستقل. وبهذا نرى أنه إذا اختلفت الكلمتان v و w في عدد d من المواقع فيكون عدد الإحداثيات المرسلة بدون أخطاء يساوي $n-d$ وعدد الإحداثيات المرسلة بأخطاء يساوي d ونحصل على:

$$\varphi_p(v,w) = p^{n-d}(1-p)^d$$

مثال (١,٦,١)

لتكن C شفرة من الطول 5 ولتكن $v \in C$. حينئذ، احتمال استقبال v دون أخطاء هو:

$$\varphi_p(v,v) = p^5$$

وإذا كانت $v = 10101 \in C$ وكانت $w = 01101$ و $p = 0.9$ فإن:

$$\varphi_p(v,w) = \varphi_p(10101,01101) = p^3(1-p)^2 = (0.9)^3(0.1)^2 = 0.00729.$$

▲

تمرين

(١,٦,٢) احسب $\varphi_{0.97}(v,w)$ لكل زوج من الكلمات v و w فيما يلي:

(أ) $v = 01101101\ , w = 10001110$

(ب) $v = 1110101\ , w = 1110101$

(ج) $v = 00101\ , w = 11010$

(د) $v = 00000\ , w = 00000$

(هـ) $v = 1011010\ , w = 0000010$

(و) $v = 10110\ , w = 01001$

(ز) $v = 111101\ \ , w = 000010$.

في التطبيق العملي نكون على معرفة بالكلمة المستقبلة w ولكننا لا نعرف كلمة الشفرة المرسلة v. كما نعلم أن كل كلمة شفرة v تُزودنا بتعيين للاحتمالات $\varphi_p(v,w)$ للكلمات المستقبلة w. كل من هذه التعينات هو نموذج رياضي وبهذا نختار النموذج (أي كلمة الشفرة v) التي تتفق مع معظم المشاهدات (في الحالة المعينة). أي نختار كلمة الشفرة التي لها احتمالية قصوى لكي تكون هي الكلمة المرسلة. وبهذا نفترض أن كلمة الشفرة v هي المرسلة عند استقبالنا للكلمة w إذا تحقق ما يلي:

$$\varphi_p(v,w) = max\{\varphi_p(u,w) : u \in C\}$$

تُزودنا المبرهنة التالية بمعيار لإيجاد كلمة الشفرة v.

مبرهنة (١,٦,٣)

لنفرض أن لدينا قناة BSC تحقق $\frac{1}{2} < p < 1$. لنفرض أن كلاً من v_1 و v_2 كلمة شفرة من الطول n وأن w كلمة طولها n. ولنفرض أن v_1 تختلف عن w بعدد d_1 من المواقع وأن v_2 تختلف عن w بعدد d_2 من المواقع. عندئذ:

$$d_2 \le d_1 \Leftrightarrow \varphi_p(v_1,w) \le \varphi_p(v_2,w)$$

البرهان

لاحظ أن

$$\begin{aligned}\varphi_p(v_1,w) \le \varphi_p(v_2,w) &\Leftrightarrow p^{n-d_1}(1-p)^{d_1} \le p^{n-d_2}(1-p)^{d_2}\\ &\Leftrightarrow \frac{p^{n-d_1}(1-p)^{d_1}}{p^{n-d_2}(1-p)^{d_2}} \le 1\\ &\Leftrightarrow \left(\frac{p}{1-p}\right)^{d_2-d_1} \le 1\\ &\Leftrightarrow d_2 \le d_1\end{aligned}$$

لأن: $\frac{p}{1-p} > 1$. ■

وبهذا نكون قد أثبتنا وجود طريقة علمية لتصويب الأخطاء ويتم ذلك على النحو التالي: إذا استقبلنا الكلمة w فإننا نقوم بتصويب w إلى كلمة الشفرة التي تختلف عنها بأقل عدد من الإحداثيات؛ لأنه غالباً ما تكون كلمة الشفرة هذه هي المرسلة.

مثال (١,٦,٤)

لنفرض أن $w = 00110$ هي الكلمة المستقبلة عبر قناة BSC حيث $p = 0.98$. بيّن أي من كلمات الشفرة التالية تكون على الأرجح قد أُرسلت:

01101 ، 01001 ، 10100 ، 10101.

الحل

v	d (عدد مواقع الاختلاف مع w)
01101	3
01001	4
10100	2 ←
10101	3

استناداً إلى الجدول السابق والمبرهنة (١,٦,٣) نجد أن كلمة الشفرة التي تكون على الأرجح قد أُرسلت هي 10100. لاحظ أننا لا نحتاج لمعرفة قيمة p الدقيقة لاستخدام المبرهنة (١,٦,٣) ولكننا فقط بحاجة لمعرفة أن $p > \frac{1}{2}$. ▲

تمارين

(١,٦,٥) لنفرض أن $w = 0010110$ هي الكلمة المستقبلة عبر قناة BSC بموثوقية $p = 0.9$. أي من كلمات الشفرة التالية تكون على الأرجح قد أُرسلت:

1101001 ، 0011001 ، 0001110 ، 1111100 ، 1001011.

(١,٦,٦) أي من كلمات الشفرة الثمانية المبينة في التمرين (١,٣,٦) هي التي تكون على الأرجح أُرسلت إذا كانت الكلمة المستقبلة هي $w = 101000101$ ؟

(١,٦,٧) إذا كانت $C = \{01000, 01001, 00011, 11001\}$ وكانت $w = 10110$ هي الكلمة المستقبلة فما هي كلمة الشفرة التي تكون على الأرجح قد أُرسلت؟

(١,٦,٨) أعد التمرين **(١,٦,٧)** إذا كانت:

$$C = \{010101, 110110, 101101, 100110, 011001\}$$

وكانت $w = 101010$.

(١,٦,٩) إذا كانت $w = 011001$ هي الكلمة المستقبلة فما هي كلمة الشفرة التي تكون على الأرجح أُرسلت من بين الكلمات التالية:

101000 ، 100111 ، 000111 ، 110101 ، 110110 ؟

(١,٦,١٠) افترضنا في المبرهنة **(١,٦,٣)** أن $\frac{1}{2} < p < 1$. ماذا يتغير في نص المبرهنة **(١,٦,٣)** لو استبدلنا الفرض ليكون:

(أ) $0 < p < \frac{1}{2}$ (ب) $p = \frac{1}{2}$.

(١,٧) بعض أساسيات الجبر

Some Basic Algebra

أحد أهدافنا هو إيجاد طريقة فعّالة لمعرفة أقرب كلمة شفرة للكلمة المستقبلة. فإذا احتوت الشفرة على عدد كبير من الكلمات فتكون طريقة مقارنة جميع كلمات الشفرة كلمة كلمة مع الكلمة المستقبلة w هي طريقة غير مجدية. على سبيل المثال، إذا كان عدد كلمات الشفرة يساوي 2^{12} (كما هو الحال في رحلات بعض المركبات الفضائية) فيكون من الصعب جداً لطريقة فك التشفير هذه (أي مقارنة الكلمات كلمة كلمة) مواكبة عملية الإرسال. وللتغلب على هذه المشكلة نعرّف بعض العمليات على الشفرات لجعلها نظاماً رياضياً.

لنفرض أن $K = \{0,1\}$ وأن K^n مجموعة جميع الكلمات الثنائية ذات الطول n.
نعرّف الجمع والضرب على K كالتالي:

$$0+0=1+1=0$$
$$0+1=1+0=1$$
$$0\cdot 0=0\cdot 1=1\cdot 0=0$$
$$1\cdot 1=1$$

ونعرّف الجمع على K^n بجمع الإحداثيات المتقابلة المعرّف على K. فمثلاً، إذا كانت $v = 01101$ و $w = 11001$ فإن:

$$v+w=01101+11001=10100$$

من الواضح أن حاصل جمع كلمتين ثنائيتين من الطول n هو كلمة ثنائية من الطول n وبهذا نرى أن K^n مغلق تحت عملية الجمع.

تُسمى عناصر K **أعداداً قياسية (Scalars)** كما هو متفق عليه في الجبر الخطي. وبهذا نعرّف الضرب بعدد قياسي على K^n بضرب كل من إحداثيات الكلمة بالعدد القياسي وحيث إن العددين القياسين هنا هما فقط 0 و 1 فنحصل على ضربين قياسين للكلمة w هما $0.w$ و $1.w$. عناصر الكلمة $0.w$ جميعها أصفار وتُسمى **الكلمة الصفرية (Zero Word)**، وأما الكلمة $1.w$ فتساوي الكلمة w نفسها. ومن الواضح أن K^n مغلق تحت عملية الضرب بعدد قياسي.

باستخدام عمليتي الجمع والضرب بعدد قياسي نستطيع وبسهولة إثبات أن K^n **فضاء متجهات (Vector Space)** أو **فضاء خطي (Linear Space)**. أي أنه يحقق الخواص التالية لكل $u, v, w \in K^n$ ولكل $a, b \in K$:

(١) $v + w \in K^n$.

(٢) $(u+v)+w = u+(v+w)$.

(٣) $v+0=0+v=v$.

(٤) يوجد $v' \in K^n$ حيث $v+v'=v'+v=0$.

(٥) $v + w = w + v$.

(٦) $av \in K^n$.

(٧) $a(v + w) = av + aw$.

(٨) $(a + b)v = av + bv$.

(٩) $(ab)v = a(bv)$.

(١٠) $1v = v$.

تمارين

(**١,٧,١**) أثبت أن $v + v = 0$ لكل $v \in K^n$.

(**١,٧,٢**) إذا كان $v, w \in K^n$ وكان $v + w = 0$ فأثبت أن $v = w$.

(**١,٧,٣**) إذا كان $u + v = w$ حيث $u, v, w \in K^n$ فأثبت أن $u + w = v$.

لنفرض أن v أُرسلت عبر قناة BSC وأن w هي الكلمة المستقبلة. إذا كان 0 هو أحد إحداثيات $v + w$ فيكون الإحداثي المقابل في الكلمة v قد أُرسل بدون خطأ. أما إذا كان 1 هو أحد إحداثيات $v + w$ فيكون قد حصل خطأ في إرسال الإحداثي المقابل في الكلمة v. تُسمى الكلمة $v + w$ **نمط الخطأ أو الخطأ** **(Error Pattern or Error)**. على سبيل المثال، إذا كانت الكلمة المرسلة هي $v = 10101$ وكانت $w = 01100$ فإن نمط الخطأ هو $v + w = 11001$ ونرى وقوع خطأ في إرسال الإحداثيات الأول والثاني والخامس.

(١,٨) الوزن والمسافة

Weight and Distance

نقدم في هذا البند مفهومين مهمين. لنفرض أن v كلمة من الطول n. يعرف **الوزن أو وزن هامينغ** **(Weight or Hamming Weight)** للكلمة v ويُرمز له بالرمز

$wt(v)$ على أنه عدد مرات ظهور الإحداثي 1 في الكلمة v. فمثلاً، $wt(110101) = 4$ و $wt(00000) = 0$.

لنفرض أن v و w كلمتان من الطول n. تُعرف **مسافة هامينغ أو المسافة** (**Hamming Distance or Distance**) بين الكلمتين v و w ويُرمز لها بالرمز $d(v,w)$ على أنها عدد المواقع المختلفة بين v و w. فمثلاً، $d(01011\,,00111) = 2$ و $d(10110\,,10110) = 0$.

لاحظ أن المسافة بين v و w تساوي وزن نمط الخطأ $u = v + w$.

أي أن:

$$d(v,w) = wt(v+w).$$

فمثلاً، إذا كانت $v = 11010$ و $w = 01101$ فإن:

$$d(v,w) = d(11010\,,01101) = 4$$

وإن $wt(v+w) = wt(11010 + 01101) = wt(10111) = 4$.

لاحظ أيضاً أنه يمكن إعادة صياغة الاحتمال المقدم في البند (**١,٦**) على النحو التالي:

$$\varphi_p(v,w) = p^{n-wt(u)}(1-p)^{wt(u)}$$

حيث $u = v + w$ هو نمط الخطأ.

نسمي $\varphi_p(u,w)$ **احتمال نمط الخطأ** (**Probability of Error Pattern**) $u = v + w$.

تمارين

(**١,٨,١**) احسب وزن كل من الكلمات التالية ثم احسب المسافة بين كل زوج منهما:

$v_1 = 1001010$ ، $v_2 = 0110101$ ، $v_3 = 0011110$ ، $v_4 = v_2 + v_3$.

(**١,٨,٢**) لنفرض أن $u = 01011$، $v = 11010$، $w = 01100$. قارن بين أزواج الكلمات فيما يلي:

(أ) $wt(v+w)$ و $wt(v) + wt(w)$

(ب) $d(v,w)$ و $d(v,u) + d(u,w)$

فيما يلي نسرد بعض خواص المسافة والوزن حيث $u, v, w \in K^n$ و $a \in K$:

(١) $0 \le wt(v) \le n$.

(٢) $wt(v) = 0$ إذا وفقط إذا كان $v = 0$.

(٣) $0 \le d(v,w) \le n$.

(٤) $d(v,w) = 0$ إذا وفقط إذا كان $v = w$.

(٥) $d(v,w) = d(w,v)$.

(٦) $wt(v+w) \le wt(v) + wt(w)$.

(٧) $d(v,w) \le d(v,u) + d(u,w)$.

(٨) $wt(av) = a \cdot wt(v)$.

(٩) $d(av,aw) = a \cdot d(v,w)$.

إثبات معظم هذه الخواص واضح من تعريف الوزن والمسافة. في التمرين (**٢,٨,١**) طلبنا من القارئ تقديم أمثلة على الحقيقتين (٦) و (٧). ولبرهان هذه الحقائق حاول استخدام العلاقة $d(v,w) = wt(v+w)$ والتمارين (**١,٧,١**)، (**١,٧,٢**)، (**١,٧,٣**) كلما دعت الحاجة إلى ذلك.

تمارين

(**١,٨,٣**) استخدم K^5 لإيجاد مثال لكل من الخواص التسع المقدمة في بداية الصفحة.

(**١,٨,٤**) أثبت جميع الخواص التسع المقدمة في بداية الصفحة.

سنستخدم هذه الخواص عند الحاجة إليها في البنود القادمة دون ذكر المرجع.

(١,٩) فك التشفير الاحتمالي الأقصى
Maximum Likelihood Decoding

نحن الآن جاهزون لمناقشة جادة لمسألتين أساسيتين في نظرية التشفير. سنفترض أننا الطرف المستقبل لقناة BSC حيث نقوم باستقبال رسالة من المرسل الموجود على

الطرف الآخر للقناة. وسنفترض أيضاً أننا الجهة التي قامت بتصميم المرسل. في الحقيقة إن مسألة تصميم المرسل هي من المسائل الأساسية.

هناك كميتان خارج سيطرتنا. أولاهما هي الاحتمال p وهو احتمال إرسال إحداثي عبر قناة BSC دون وقوع خطأ وأما الكمية الثانية فهي عدد الرسائل الممكن إرسالها. في الحقيقة، الرسائل الأصلية ليست بأهم من عدد الرسائل الممكن إرسالها. على سبيل المثال، احتاج **بول ريفير (Paul Revere)** إلى رسالتين فقط قبل قيامه برحلة منتصف الليل المشهورة (سافر بول ريفير بتاريخ ١٧٧٥/٤/١٨م من بوسطن إلى لكسنغتون لتحذير كل من صاموئيل آدمز وجون هانكوك من نية القوات البريطانية لمحاولة اعتقالهم ووصل في الوقت المناسب)[١].

تذكر أن $|S|$ يرمز لعدد عناصر S. ولذا فإن $|K^n| = 2^n$ كما هو مبين في التمرين (**١,٢,٢**). المسألتان الأساسيتان في التشفير هما:

(١,٩,١) التشفير (Encoding)

المطلوب هنا هو تحديد شفرة لغرض استخدامها في إرسال رسائلنا. ولهذا نختار عدداً صحيحاً موجباً k ليكون طول الكلمة الثنائية المقابلة للرسالة المزمع إرسالها. وبما أن الرسائل المختلفة تقابل كلمات ثنائية طول كل منها k فيجب أن نختار k ليحقق $|M| \leq |K^k| = 2^k$.

بعد الانتهاء من اختيار k نقوم بتحديد عدد الإحداثيات المراد إضافتها لكل كلمة من الطول k لضمان تصويب واكتشاف جميع الأخطاء التي نأمل من شفرتنا اكتشافها وتصويبها وهذا هو اختيار كلمات الشفرة وطول الشفرة وليكن n. الآن، لإرسال رسالة معينة يقوم المرسل بإيجاد الكلمة الثنائية من الطول k المقابلة للرسالة

---

(١) المترجمان

ومن ثم إضافة $n-k$ إحداثياً إليها وإرسال كلمة الشفرة ذات الطول n المقابلة للكلمة ذات الطول k.

(١,٩,٢) فك التشفير (Decoding)

نفرض أننا استقبلنا كلمة $w \in K^n$. نُقدم الآن وصفاً لطريقة تُدعى **فك التشفير الاحتمالي الأقصى (Maximum Likelihood Decoding) أو اختصاراً MLD** لتحديد أي من كلمات الشفرة $v \in C$ قد تم إرسالها. يوجد نوعان من MLD هما :

(١) فك التشفير الاحتمالي الأقصى التام (Complete Maximum Likelihood Decoding) أو اختصاراً CMLD يتم فك التشفير في هذا النوع على النحو التالي : إذا وجدت كلمة شفرة وحيدة $v \in C$ هي الأقرب إلى الكلمة المستقبلة w من جميع كلمات الشفرة الأخرى فنعتبر v هي فك تشفير w. أي أنه إذا كان $d(v,w) < d(v_1,w)$ لكل $v_1 \in C$ حيث $v_1 \neq v$ فإن v هي فك تشفير w (أي نعتبر أن v هي كلمة الشفرة المرسلة). أما إذا وجدت عدة كلمات شفرة $v_1, v_2, \cdots, v_k \in C$ تُحقق $d(v_1,w) = d(v_2,w) = \cdots = d(v_k,w)$ وأن $d(v_i,w) < d(u,w)$ لكل $u \in C$ و $v_i \neq u$ فنأخذ أي كلمة v_i من $v_1, v_2, \cdots, v_k$ على أنها فك تشفير w (أي أن v_i هي الكلمة المرسلة).

(٢) فك التشفير الاحتمالي الأقصى غير التام (Incomplete Maximum Likelihood Decoding) أو اختصاراً IMLD يتم فك التشفير في هذا النوع على النحو التالي : إذا وجدت كلمة شفرة وحيدة $v \in C$ هي الأقرب إلى w من جميع كلمات الشفرة الأخرى فتأخذ v لتكون فك تشفير w. أما إذا وجدت عدة كلمات شفرة جميعها تبعد المسافة نفسها عن w والأقرب إلى w من جميع كلمات الشفرة الأخرى فنقوم بطلب إعادة إرسال. وفي بعض الحالات نطلب إعادة إرسال إذا وجدنا أن الكلمة المرسلة w بعيدة عن جميع كلمات الشفرة.

في أمثلة وتمارين هذا البند وفي معظم هذا الكتاب، نستخدم IMLD لفك التشفير. ونريد أن نؤكد على أن طريقة MLD تفشل في بعض الأحيان خاصة إذا وقعت أخطاء كثيرة أثناء الإرسال عبر قناة BSC.

تكون كلمة الشفرة $v \in C$ الأقرب إلى الكلمة المستقبلة w عندما تكون المسافة $d(v,w)$ صغرى، ونرى استناداً إلى المبرهنة (**١,٦,٣**) أن الاحتمال المقرون $\varphi_p(v,w)$ أعظمي، وبهذا تكون v هي على الأرجح كلمة الشفرة المرسلة وهذا موضح في المثال (**١,٦,٤**). وبما أن $d(v,w) = wt(v+w)$ هو وزن نمط الخطأ $u = v + w$ فمن الممكن إعادة صياغة المبرهنة (**١,٦,٣**) لتكون:

$\varphi_p(v_1,w) \le \varphi_p(v_2,w)$ إذا وفقط إذا كان $wt(v_1+w) \ge wt(v_2+w)$.

وهذا يعني أن الكلمة المرسلة ذات نمط خطأ وزنه أصغري.

وبهذا نرى أن الإستراتيجية المتبعة في طريقة IMLD هي اختبار أنماط الأخطاء $v + w$ لكل كلمة شفرة v ومن ثم اختيار كلمة الشفرة v التي تؤدي إلى نمط خطأ وزنه أصغري.

مثال (١,٩,٣)

لنفرض أن $|M| = 2$ (أي أن $k = 1$) وأننا اخترنا $n = 3$ و $C = \{000, 111\}$. إذا كانت $v = 000$ هي كلمة الشفرة المرسلة فبيّن متى يكون فك التشفير بطريقة IMLD صحيحاً (أي استنتاج أن $v = 000$ هي فعلاً كلمة الشفرة المرسلة) ومتى يكون استنتاج IMLD أن 111 هي الكلمة المرسلة (أي أن يكون الاستنتاج خاطئاً).

الحل

نقوم بإنشاء الجدول (١,١) على النحو التالي:

الجدول (١,١). جدول IMLD للمثال (١,٩,٣).

الكلمات المستقبلة	أنماط الأخطاء		فك التشفير (التصويب)[٢]
w	$000+w$	$111+w$	v
000	000*	111	000
100	100*	011	000
010	010*	101	000
001	001*	110	000
110	110	001*	111
101	101	010*	111
011	011	100*	111
111	111	000*	111

العمود الأول من الجدول (١,١) يُبيّن جميع الكلمات الممكن استقبالها وهذه جميع عناصر K^3. العمودان الثاني والثالث يبينان أنماط الأخطاء $v+w$ لكل كلمة شفرة $v \in C$. وبما أن طريقة IMLD تختار نمط الخطأ الأصغر وزناً فقمنا بمقارنة أوزان أنماط الأخطاء في العمودين الثاني والثالث ووضعنا علامة * بمحاذة نمط الوزن الأصغر. وأخيراً وضعنا في العمود الأخير الكلمة $v \in C$ التي يكون عمود نمط الخطأ $v+w$ لها معلماً بالعلامة *. وهذه هي كلمة الشفرة v التي تستنتج طريقة IMLD أنها قد أُرسلت عند استقبال الكلمة w المقابلة لها. وبهذا يكون فك تشفير كل من الكلمات المرسلة 000 ، 100 ، 010 ، 001 بطريقة IMLD هي كلمة الشفرة 000 (وهذا استنتاج صائب) وفك تشفير كل من الكلمات المرسلة 110 ، 101 ، 011 ، 111 هي كلمة الشفرة 111 (وهذا استنتاج خاطئ). ▲

(٢) المترجمان: ننبّه القارئ إلى أن التعبير "فك التشفير" المستخدم في هذا الكتاب يعني تصويب الخطأ ويرجع سبب استخدام المؤلفون للتعبير "فك التشفير" عوضاً عن "تصويب الخطأ" إلى تعود مهندسي الاتصالات على هذا الاستخدام للمصطلح. وسنتبنى التعبير الذي استخدمه المؤلفون لهذا المصطلح.

مثال (١,٩,٤)

في هذا المثال نفرض أن $|M| = 3$ وأن $n = 4$ وأن $C = \{0000\,,1010\,,0111\}$. نقوم بإنشاء جدول IMLD بطريقة مشابهة للمثال (**١,٩,٣**)، والخلاف الوحيد هنا هو أنه إذا وجد أكثر من نمط خطأ واحد ذي وزن أصغري فإننا لن نضع علامة * في الصف الذي يحتوي على هذه الأنماط ونضع العلامة — (تعني لا شيء) في عمود فك التشفير لهذا الصف. هذا يعني أن طريقة IMLD لفك التشفير تطلب إعادة إرسال عند وجود أكثر من نمط خطأ له الوزن الأصغر.

الجدول (١,٢). جدول IMLD للمثال (١,٩,٤).

فك التشفير	أنماط الأخطاء			الكلمات المستقبلة
v	$0000 + w$	$1010 + w$	$0111 + w$	w
0000	0111	1010	0000*	0000
–	1111	0010	1000	1000
0000	0011	1110	0100*	0100
–	0101	1000	0010	0010
0000	0110	1011	0001*	0001
–	1011	0110	1100	1100
1010	1101	0000*	1010	1010
–	1110	0011	1001	1001
0111	0001*	1100	0110	0110
0111	0010*	1111	0101	0101
0111	0100*	1001	0011	0011
1010	1001	0100*	1110	1110
0111	1010*	0111	1101	1101
1010	1100	0001*	1011	1011
0111	0000*	1101	0111	0111
0111	1000*	0101	1111	1111

▲

تمارين

(**١,٩,٥**) لنفرض أن $|M| = 2$، $n = 3$، $C = \{001\,,101\}$. إذا كانت $v = 001$ هي كلمة الشفرة المرسلة فمتى يكون استنتاج طريقة IMLD صائباً بأن v هي المرسلة ومتى يكون استنتاج طريقة IMLD خاطئاً بأن 101 هي الكلمة المرسلة ؟

(١,٩,٦) لنفرض أن $|M| = 3$ ، $n = 3$. لكل كلمة مرسلة $w \in K^3$ جد كلمة الشفرة v في الشفرة $C = \{000, 001, 110\}$ التي تستنتج طريقة IMLD أنها قد أُرسلت.

(١,٩,٧) أنشئ جدول IMLD لكل من الشفرات التالية :

(أ) $C = \{101, 111, 011\}$

(ب) $C = \{000, 001, 010, 011\}$

(ج) $C = \{0000, 0001, 1110\}$

(د) $C = \{0000, 1001, 0110, 1111\}$

(هـ) $C = \{00000, 11111\}$

(و) $C = \{00000, 11100, 00111, 11011\}$

(ز) $C = \{00000, 11110, 01111, 10001\}$

(ح) $C = \{000000, 101010, 010101, 111111\}$

بيّنا في البند الجزئي (١,٩,١) أنه يجب علينا اختيار n و C. ولذا تكون بعض الخيارات أفضل من غيرها. نسرد هنا ثلاثة معايير مهمة لقياس الخيارات الجيدة :

(١) كلما ازداد طول الكلمة ازداد الزمن اللازم للإرسال وفك التشفير. وبهذا لا ينصح باختيار عدد كبير n. أي أن معدل المعلومات يجب أن يكون أقرب إلى 1 كلما أمكن ذلك.

(٢) إذا كان عدد الرسائل المرسلة كبيراً (مثلاً $|C|$ يساوي بضعة آلاف) فإن ذلك يستغرق زمناً كبيراً لتنفيذ طريقة IMLD. ولذا فالاختيار المدروس للشفرة C يؤدي إلى طرق ماهرة وسريعة لتنفيذ IMLD.

(٣) إذا وقعت أخطاء كثيرة أثناء عملية الإرسال فلا يصلح استخدام طريقة MLD في فك التشفير ؛ وذلك لأن الكلمة التي تَدّعي MLD أنها قد أُرسلت هي ليست

الكلمة المرسلة بالفعل، ولهذا يجب علينا عند استخدام MLD اختيار الشفرة C بحيث يكون احتمال نجاح MLD كبير جداً (سنناقش هذا الاحتمال في البند التالي).

نستطيع القول، بناء على ما تقدم، إن الهدف الرئيس لنظرية التشفير هو إيجاد شفرات C تناسب المعايير الثلاث السابقة. وسيكون معظم جهدنا مركزاً لتحقيق هذا الهدف.

(١,١٠) موثوقية MLD
Reliability of MLD

لنفرض أنه قد تم اختيار كل من n و C. ولنفرض أن BSC قناة ذات احتمال p ولنفرض أن $\theta_p(C,v)$ هو احتمال استنتاج IMLD صواباً بأن v هي الكلمة التي أُرسلت. سنقدم الآن طريقة لحساب $\theta_p(C,v)$.

لتكن $L(v) = \{w \in K^n : d(w,v) < d(w,u) \quad \forall u \in C, u \neq v\}$. أي أن $L(v)$ هي مجموعة كلمات K^n الأقرب إلى v منها إلى أي كلمة من الكلمات الأخرى للشفرة C. لاحظ أيضاً أن $L(v)$ هي بالضبط مجموعة الكلمات من K^n التي إذا استقبلت فإن IMLD تستنتج صواباً أن v هي بالفعل الكلمة المرسلة. عندئذ، نجد أن:

$$\theta_p(C,v) = \sum_{w \in L(v)} \varphi_p(v,w)$$

من الممكن إيجاد $L(v)$ من جدول IMLD المبين في البند السابق وذلك كما يلي:

في كل صف من صفوف الجدول الذي يحتوي فك التشفير v في عموده الأخير تنتمي الكلمة $w \in K^n$ الواقعة في العمود الأول لهذا الصف تنتمي إلى $L(v)$. وهذه هي جميع كلمات $L(v)$.

لاحظ أيضاً أن $\theta_p(C,v)$ هي مجموع الاحتمالات المأخوذ على الكلمات $w \in L(v)$ بحيث يكون نمط الخطأ الذي تم وقوعه أثناء الإرسال هو $v + w$.

من الممكن استخدام θ_p لمقارنة شفرتين واختيار الشفرة الأفضل منهما (التي تحقق المعيار (٣) من المعايير المقدمة في البند السابق)، مع ملاحظة أن $\theta_p(C,v)$ تتجاهل إمكانية إعادة الإرسال عند تساوي المسافتين بين الكلمة المرسلة وكلمتي شفرة، وهذا يؤدي في بعض الأحيان إلى الخروج عن المألوف (فمثلاً، $\theta_p(K^n,v) > \theta_p(C,v)$ لكل $v \in K^n$ ولكل $u \in C$ حيث C شفرة اختبار النوعية المكوّنة من K^n)، ومع ذلك فهو تقريب أولي مناسب لقياس الموثوقية. من المؤكد أيضاً أن $\theta_p(C,v)$ هو حد أدنى لاحتمال فك تشفير v بشكل صائب.

مثال (١,١٠,١)

لنفرض أن $p = 0.9$ ، $|M| = 2$ ، $n = 3$ ، $C = \{000\,,111\}$ كما هو مبين في المثال (**١,٩,٣**). احسب احتمال أن تكون طريقة IMLD قد استنتجت صواباً أن v هي بالفعل الكلمة التي تم إرسالها بعد عملية إرسال واحدة إذا كانت:

(أ) $v = 000$ (ب) $v = 111$.

الحل

(أ) باستخدام الجدول (**١,١**) نجد أن $v = 000$ هي فك التشفير في الصفوف الأربعة الأولى ونرى أن $L(000)$ (مجموعة كلمات K^3 الأقرب إلى $v = 000$ منها إلى 111) هي:

$$L(000) = \{000\,,100\,,010\,,001\}$$

وبهذا يكون:

$$\begin{aligned}\theta_p(C,000) &= \varphi_p(000{,}000) + \varphi_p(000{,}100) + \varphi_p(000{,}010) + \varphi_p(000{,}001)\\ &= p^3 + p^2(1-p) + p^2(1-p) + p^2(1-p)\\ &= p^3 + 3p^2(1-p)\\ &= .972 \quad (\text{على فرض أن } p = 0.9)\end{aligned}$$

(ب) إذا كانت $v = 111$ فنجد في هذه الحالة أن:

$$L(111) = \{110\,,101\,,011\,,111\}$$

ونرى أن:

$$\begin{aligned}\theta_p(C,111) &= \varphi_p(111\,,110) + \varphi_p(111\,,101) + \varphi_p(111,011) + \varphi_p(111\,,111)\\ &= p^2(1-p) + p^2(1-p) + p^2(1-p) + p^3\\ &= 3p^2(1-p) + p^3\\ &= .972 \quad (\text{على فرض أن } p = 0.9)\end{aligned}$$

▲

تمرين

(**١,١٠,٢**) لنفرض أن $p = 0.9$، $|M| = 2$، $n = 3$، $C = \{001\,,101\}$ كما هو مبيّن في التمرين (**١,٩,٥**).

(أ) إذا كانت $v = 001$ هي الكلمة المرسلة فاحسب احتمال أن تكون طريقة IMLD قد استنتجت صواباً أن v هي بالفعل الكلمة التي تم إرسالها بعد عملية إرسال واحدة.

(ب) أعد الفقرة (أ) للكلمة $v = 101$.

إجابة التمرين (**١,١٠,٢**) في كلتا الحالتين هي $\theta_p(C,v) = 0.900$. وبمقارنة ذلك مع نتيجة المثال (**١,١٠,١**) نجد أن الشفرة $C = \{000\,,111\}$ أفضل من الشفرة $C = \{001\,,101\}$ (لأن $0.972 > 0.900$) على الأقل من وجهة نظر المعيار (**٣**) المقدّم في البند السابق. بناء على ما تقدم نستطيع القول (على الأقل عندما يكون n عدداً صغيراً) إن حساب الاحتمال يُزودنا بمعرفة الحالات التي تكون فيها نتائج طريقة IMLD مرضية. ولحسن الحظ ستكون حسابات الاحتمالات لمعظم الشفرات التي سندرسها لاحقاً أكثر سهولة.

مثال (٣,١٠,١)

لنفرض أن $p = 0.9$ ، $|M| = 3$ ، $n = 4$ ، $C = \{0000\,, 1010\,, 0111\}$ كما هو مبين في المثال (١,٩,٤). لكل $v \in C$ احسب $\theta_p(C, v)$.

الحل

(أ) في حالة $v = 0000$ لدينا :

$L(0000) = \{0000\,, 0100\,, 0001\}$ (من الجدول (١,٢))

$$\begin{aligned}\theta_p(C,v) &= \varphi_p(0000\,,0000) + \varphi_p(0000\,,0100) + \varphi_p(0000\,,0001)\\ &= p^4 + p^3(1-p) + p^3(1-p)\\ &= p^4 + 2p^3(1-p) = .8019\end{aligned}$$

(ب) إذا كان $v = 1010$ فإن :

$$L(1010) = \{1010\,, 1110\,, 1011\}$$

$$\begin{aligned}\theta_p(C,v) &= \varphi_p(1010\,,1010) + \varphi_p(1010\,,1110) + \varphi_p(1010\,,1011)\\ &= p^4 + p^3(1-p) + p^3(1-p)\\ &= p^4 + 2p^3(1-p) = .8019\end{aligned}$$

(ج) وأخيراً في الحالة $v = 0111$ يكون :

$$L(0111) = \{0110\,, 0101\,, 0011\,, 1101\,, 0111\,, 1111\}$$

$$\begin{aligned}\theta_p(C,v) &= \varphi_p(0111\,,0110) + \varphi_p(0111\,,0101) + \varphi_p(0111\,,0011)\\ &\quad + \varphi_p(0111\,,1101) + \varphi_p(0111\,,0111) + \varphi_p(0111\,,1111)\\ &= p^3(1-p) + p^3(1-p) + p^3(1-p) + p^2(1-p)^2 + p^4 + p^3(1-p)\\ &= p^4 + 4p^3(1-p) + p^2(1-p)^2 = .9558\end{aligned}$$

بالتمحيص في هذه الاحتمالات نجد أن احتمال أن تكون طريقة IMLD قد استنتجت صواباً أن الكلمة 0111 هي المرسلة ليس سيئاً. ولكن احتمال أن تكون قد استنتجت صواباً أن الكلمة 0000 أو الكلمة 1010 هي الرسالة فهو سيء للغاية. وبهذا نستنتج (على الأقل من المعيار الثالث المقدم في البند السابق) أن اختيار $C = \{0000\,, 1010\,, 0111\}$ ليس بالاختيار المناسب لشفرة. ▲

تمارين

(**١,١٠,٤**) لنفرض أن $p = 0.9$ وأن $C = \{000\,,001\,,110\}$ كما هو مبين في التمرين (**١,٩,٦**). إذا كانت $v = 110$ هي الكلمة المرسلة فاحسب احتمال أن تكون طريقة IMLD استنتجت صواباً أن v هي بالفعل الكلمة المرسلة واحسب احتمال أن تكون طريقة IMLD استنتجت خطأ أن الكلمة 000 هي المرسلة.

(**١,١٠,٥**) لكل من الشفرات C أدناه، احسب $\theta_p(C,v)$ لكل $v \in C$ مستخدماً $p = 0.9$ (جداول IMLD لهذه الشفرات قد تم إنشاؤها في التمرين (**١,٩,٧**)):

(أ) $C = \{101\,,111\,,011\}$

(ب) $C = \{000\,,001\,,010\,,011\}$

(ج) $C = \{0000\,,0001\,,1110\}$

(د) $C = \{0000\,,1001\,,0110\,,1111\}$

(هـ) $C = \{00000\,,11111\}$

(و) $C = \{00000\,,11100\,,00111\,,11011\}$

(ز) $C = \{00000\,,11110\,,01111\,,10001\}$

(ح) $C = \{000000\,,101010\,,010101\,,111111\}$.

(**١,١١**) شفرات اكتشاف الأخطاء

Error-Detecting Codes

في هذا البند نعرّف بشكل دقيق متى يكون بمقدور شفرة C اكتشاف الأخطاء. تذكر أنه إذا كانت $v \in C$ هي الكلمة المرسلة وكانت $w \in K^n$ هي الكلمة المستقبلة فإن $u = v + w$ هو نمط الخطأ. لاحظ أيضاً أن أي كلمة $u \in K^n$ ممكن أن تكون نمط خطأ والمطلوب هو معرفة أي من أنماط الأخطاء تستطيع الشفرة C اكتشافها.

نقول إن الشفرة C **تكتشف (Detects)** نمط الخطأ u إذا وفقط إذا كان $v + u \notin C$ لكل $v \in C$. أي أن C تستطيع اكتشاف نمط الخطأ u إذا تحقق ما يلي :

بعد إرسال كلمة الشفرة v واستقبال $v + u$ يكون بإمكان **فاكك التشفير (Decoder)** التحقق من أن $v + u$ ليست كلمة شفرة ومن ثم فهناك خطأ ما قد وقع.

مثال (١,١١,١)

لنفرض أن $C = \{001, 101, 110\}$. بيّن أن C تكتشف نمط الخطأ $u = 010$ ولكنها لا تكتشف نمط الخطأ $u = 100$.

الحل

إذا كان $u = 010$ فنقوم بحساب $v + 010$ لكل $v \in C$ فنجد :

$$001 + 010 = 011 \notin C$$
$$101 + 010 = 111 \notin C$$
$$110 + 010 = 100 \notin C$$

وبهذا نرى أن C تكتشف $u = 010$. وبحساب $v + 100$ لكل $v \in C$ نجد :

$$001 + 100 = 101 \in C$$
$$101 + 100 = 101 \in C$$
$$110 + 100 = 010 \notin C$$

وبما أن واحداً على الأقل من هذه المجاميع ينتمي إلى C فنرى أن C لا تكتشف نمط الخطأ $u = 100$. ▲

تمارين

(**١,١١,٢**) لنفرض أن $C = \{001, 101, 110\}$. بيّن ما إذا كان بإمكان C إكتشاف أي من أنماط الأخطاء التالية :

(أ) 011 (ب) 001 (ج) 000

(**١,١١,٣**) لكل من الشفرات التالية C بيّن فيما إذا كان بإمكان C اكتشاف نمط الخطأ u المعطى :

(أ) $C = \{00000, 10101, 00111, 11100\}$

(i) $u = 10101$
(ii) $u = 01010$
(iii) $u = 1010$

(ب) $C = \{1101, 0110, 1100\}$

(i) $u = 0010$
(ii) $u = 0011$
(iii) $u = 1010$

(ج) $C = \{1000, 0100, 0010, 0001\}$

(i) $u = 1001$
(ii) $u = 1110$
(iii) $u = 0110$

(**١,١١,٤**) أي من أنماط الأخطاء تستطيع الشفرة $C = K^n$ اكتشافها ؟

(**١,١١,٥**) (أ) لتكن C شفرة تحتوي الكلمة الصفرية. أثبت أنه إذا كان نمط الخطأ u هو كلمة شفرة فليس بإمكان C اكتشاف u.

(ب) أثبت عدم وجود شفرات يكون بإمكانها اكتشاف نمط الخطأ $u = 0$.

من الممكن استخدام جدول IMLD لمعرفة أنماط الأخطاء التي تستطيع الشفرة C اكتشافها. فالعمود الأول يسرد جميع كلمات K^n ومن ثم يمكن النظر إليه على أنه جميع أنماط الأخطاء الممكنة، وبذلك تكون أعمدة أنماط الأخطاء في الجدول هي المجموع $v + u$ لكل $v \in C$. الآن، إذا لم ينتم أي من هذه المجاميع في صف ما إلى الشفرة C فإن C تكتشف نمط الخطأ الواقع في العمود الأول من ذلك الصف.

مثال (١,١١,٦)

لنفرض أن $C = \{000, 111\}$ هي الشفرة حيث جدول IMLD لها هو الجدول (**١,١**). العمود الأول يحتوي على جميع أنماط الأخطاء u الممكنة. ولكل u نجد أن

جميع المجاميع $v+u$ لكل $v \in C$ هي الموجودة في العمودين الثاني والثالث. فإذا كانت جميع هذه المجاميع لا تنتمي إلى C (أي لا تساوي 000 أو 111) فإن C يكتشف u. وبهذا نرى أن C تكتشف أنماط الأخطاء 100 ، 010 ، 001 ، 110 ، 101 ، 011 وذلك بالنظر إلى الأعمدة من 2 إلى 7، ولكن لا تستطيع C إكتشاف أي من الخطأين 000 أو 111. ▲

تمرين

(**١,١١,٧**) استخدم جدول IMLD للشفرة C المنشأ في التمرين (**١,٩,٧**) لإيجاد أنماط الأخطاء التي تستطيع C اكتشافها.

طريقة أخرى ولكنها أسرع كثيراً لإيجاد أنماط الأخطاء التي يمكن لشفرة C اكتشافها تكون بإيجاد أنماط الأخطاء التي لا تستطيع C اكتشافها ومن ثم فإن C تكتشف جميع أنماط الأخطاء المتبقية. من الواضح أنه إذا كانت $v,w \in C$ وكان $e = v + w$ فلا تستطيع C اكتشاف e ؛ وذلك لأن $v + e = w \in C$. وبهذا نرى أن أنماط الأخطاء التي لا تتمكن C من اكتشافها هي مجموعة جميع الكلمات التي يمكن كتابتها كمجموع كلمتي شفرة.

مثال (١,١١,٨)

لنفرض أن $C = \{000\,,111\}$ شفرة. بملاحظة أن

$$000 + 000 = 000$$
$$000 + 111 = 111$$
$$111 + 111 = 000$$

نجد أن مجموعة أنماط الأخطاء التي لا تكتشفها C هي $\{000\,,111\}$. وبهذا فإن مجموعة أنماط الأخطاء التي تستطيع C اكتشافها هي $K^3\backslash\{000\,,111\}$. ▲

مثال (١,١١,٩)

لنفرض أن $C = \{1000\,, 0100\,, 1111\}$ شفرة. بما أن:

$$1000 + 1000 = 0000$$
$$1000 + 0100 = 1100$$
$$1000 + 1111 = 0111$$
$$0100 + 1111 = 1011$$

فنجد أن مجموعة أنماط الأخطاء التي لا تستطيع C اكتشافها هي $\{0000\,, 1100\,, 0111\,, 1011\}$ وبهذا تكون مجموعة أنماط الأخطاء التي يتم اكتشافها بواسطة C هي $K^4\backslash\{0000\,, 1100\,, 0111\,, 1011\}$. ▲

تمرين

(**١,١١,١٠**) جد مجموعة أنماط الأخطاء التي يمكن اكتشافها بواسطة كل من الشفرات التالية ثم قارن إجاباتك مع إجابات التمرين (**١,١١,٧**):

(أ) $C = \{101\,, 111\,, 011\}$

(ب) $C = \{000\,, 001\,, 010\,, 011\}$

(ج) $C = \{0000\,, 0001\,, 1110\}$

(د) $C = \{0000\,, 1001\,, 0110\,, 1111\}$

(هـ) $C = \{00000\,, 11111\}$

(و) $C = \{00000\,, 11100\,, 00111\,, 11011\}$

(ز) $C = \{00000\,, 11110\,, 01111\,, 10001\}$

(ح) $C = \{000000\,, 101010\,, 010101\,, 111111\}$.

سنبين الآن طريقة أخرى لتحديد بعض أنماط الأخطاء التي تستطيع شفرة C اكتشافها بدون الحاجة إلى إجراء الحسابات الطويلة ولكننا نقدم أولاً عدداً آخر يقترن بالشفرة C.

إذا كانت C شفرة تحتوي كلمتين على الأقل فتعرّف مسافة $\boldsymbol{C}$ **(Distance of $\boldsymbol{C}$)** على أنها أصغر مسافة $d(v,w)$ لكل $v,w \in C$ حيث $v \neq w$. وبما أن $d(v,w) = wt(v+w)$ فتكون مسافة الشفرة C أصغر الأوزان $wt(v+w)$ لكل $v,w \in C$ حيث $v \neq w$.

تشترك مسافة الشفرة مع المسافة الاقليدية بالعديد من الخواص وهذا يساعد على فهم مفهوم مسافة الشفرة.

مثال (**١,١١,١١**)

إذا كانت $C = \{0000\,, 1010\,, 0111\}$ فإن:

$$d(0000\,, 1010) = 2$$
$$d(0000\,, 0111) = 3$$
$$d(1010\,, 0111) = 3$$

وبهذا تكون مسافة الشفرة C تساوي 2. ▲

تمارين

(**١,١١,١٢**) احسب مسافة كل من الشفرات التالية:

(أ) $C = \{101\,, 111\,, 011\}$

(ب) $C = \{000\,, 001\,, 010\,, 011\}$

(ج) $C = \{0000\,, 0001\,, 1110\}$

(د) $C = \{0000\,, 1001\,, 0110\,, 1111\}$

(هـ) $C = \{00000\,, 11111\}$

(و) $C = \{00000\,, 11100\,, 00111\,, 11011\}$

(ز) $C = \{00000\,, 11110\,, 01111\,, 10001\}$

(ح) $C = \{000000\,, 101010\,, 010101\,, 111111\}$

(**١,١١,١٣**) احسب مسافة الشفرة التي نحصل عليها بإضافة إحداثي اختبار النوعية للمجموعة K^n.

المبرهنة التالية تساعدنا على معرفة الكثير من أنماط الأخطاء التي يمكن لشفرة اكتشافها.

مبرهنة (١,١١,١٤)

تستطيع شفرة C مسافتها d اكتشاف على الأقل جميع أنماط الأخطاء غير الصفرية التي وزنها لا يزيد عن $d - 1$. إضافة إلى ذلك يوجد على الأقل نمط خطأ واحد وزنه d لا تتمكن الشفرة C من اكتشافه.

البرهان

لنفرض أن u نمط خطأ غير صفري حيث $wt(u) \leq d - 1$. ولنفرض أن $v \in C$. عندئذ:

$$d(v, v + u) = wt(v + v + u) = wt(u) < d.$$

وبما أن مسافة C تساوي d فإن $v + u \notin C$ وبهذا تستطيع C اكتشاف u. من تعريف المسافة d، نرى وجود كلمتين $v, w \in C$ حيث $d(v, w) = d$. لنفرض أن $u = v + w$ نمط خطأ. عندئذ، $w = v + u \in C$ ومن ثم C لا تكتشف نمط الخطأ u ذا الوزن d. ■

ملحوظة

لاحظ إمكانية اكتشاف الشفرة C لأنماط أخطاء وزنها أكبر من أو يساوي d ولكنها لا تستطيع اكتشاف جميع أنماط الأخطاء ذات الوزن d.

نقول إن شفرة C من الدرجة t في اكتشاف الأخطاء (**t Error-Detecting Code**) إذا تمكنت من اكتشاف جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن t ولكنها لا تكتشف على الأقل نمط خطأ واحد وزنه $t + 1$. وبهذا نرى استناداً إلى المبرهنة (**١,١١,١٤**) أن الشفرة C ذات المسافة d هي شفرة تكتشف أنماط أخطاء من النوع $d - 1$.

مثال (١,١١,١٥)

مسافة الشفرة $C = \{000\,,111\}$ تساوي $d = 3$. واستناداً إلى المبرهنة (**١,١١,١٤**) نرى أن C تكتشف جميع أنماط الأخطاء ذات الوزن 1 أو الوزن 2 وأن C لا تكتشف نمط الخطأ الوحيد 111 ذا الوزن 3. نمط الخطأ الوحيد الذي لا نستطيع تطبيق المبرهنة (**١,١١,١٤**) عليه هو 000 ولكننا رأينا في التمرين (**١,١١,١٥**) أن نمط الخطأ هذا لا يمكن اكتشافه. ▲

كما أسلفنا فالمبرهنة (**١,١١,١٤**) لا تمنع شفرة C من اكتشاف أنماط أخطاء وزنها d أو أكثر. في العادة، C تكتشف بعض أنماط أخطاء ذات أوزان أكبر من أو تساوي d.

مثال (١,١١,١٦)

مسافة الشفرة $C = \{001\,,101\,,110\}$ هي $d = 1$. بما أن $d - 1 = 0$ فلا نستطيع استخدام المبرهنة (**١,١١,١٤**) لاكتشاف أنماط الأخطاء ولكنها تضمن لنا وجود نمط خطأ واحد على الأقل وزنه $d = 1$ لا تستطيع C اكتشافه. وكما رأينا في المثال (**١,١١,١**) فنمط الخطأ 100 مثال لذلك. لاحظ أيضاً أن C لا تكتشف نمط الخطأ 010 حيث وزنه 1 أيضاً. ▲

تمارين

(**١,١١,١٧**) مسافة الشفرة $C = \{0000\,,1010\,,0111\}$ هي $d = 2$. استخدم التمرين (**١,١١,٥**) لإثبات أن C لا تكتشف نمط الخطأ 1010. أثبت أيضاً أن نمط الخطأ هذا هو الوحيد ذو الوزن 2 الذي لا يمكن اكتشافه بواسطة C. جد جميع أنماط الأخطاء التي تستطيع C إكتشافها.

(**١,١١,١٨**) جد جميع أنماط الأخطاء التي تستطيع الشفرة C_3 المقدمة في المثال (**١,٣,٣**) اكتشافها. لاحظ أن C_3 تكتشف أنماط أخطاء من النوع 1.

(**١,١١,١٩**) لكل شفرة C من شفرات التمرين (**١,١١,١٢**) جد جميع أنماط الأخطاء المضمون اكتشافها من قبل C بتطبيق المبرهنة (**١,١١,١٤**).

(**١,١١,٢٠**) لنفرض أن C هي الشفرة التي تحتوي جميع الكلمات ذات الطول 4 وذات الوزن الزوجي. عيّن جميع أنماط الأخطاء التي يمكن اكتشافها من قبل C.

(١,١٢) شفرات تصويب الأخطاء
Error-Correcting Codes

لنفرض أنه قد تم إرسال كلمة الشفرة $v \in C$ عبر قناة BSC ولنفرض أن w هي الكلمة المستقبلة ولنفرض أنه قد وقع نمط الخطأ $u = v + w$ أثناء عملية الإرسال. عندئذ، يكون استنتاج طريقة IMLD صائباً بأن v هي بالفعل الكلمة المرسلة إذا كانت w أقرب إلى v من أي كلمة شفرة أخرى. وإذا حصل هذا في كل مرة يقع فيها نمط الخطأ u بغض النظر عن الكلمة المرسلة فنقول إن **C تصوّب نمط الخطأ u** (**C Corrects the Error-Pattern u**). أي أن C تصوّب نمط الخطأ u إذا كان لكل $v \in C$، $v + u$ أقرب إلى v من أي من كلمات الشفرة C الأخرى. ومن الممكن صياغة ذلك رياضياً بقولنا إن C تصوّب نمط الخطأ u إذا تحقق ما يلي:

$$\forall\ v \in C\ ,\forall\ w \in C(v \neq w \rightarrow d(v, v+u) < d(w, v+u)$$

ونقول إن الشفرة C **من الدرجة t في تصويب الأخطاء** (**t Error-Correcting Code**) إذا كانت C تصوّب جميع أنماط الأخطاء ذات الوزن t ولا تصوّب نمط خطأ واحد على الأقل وزنه $t + 1$.

مثال (١,١٢,١)

لنفرض أن $C = \{000\ ,111\}$.

(أ) أثبت أن C تصوّب نمط الخطأ $u = 010$.

(ب) أثبت أن C لا تصوّب نمط الخطأ $u = 110$.

الحل

(أ) عند $v = 000$ لدينا :

$$d(000, v+u) = d(000,010) = 1$$
$$d(111, v+u) = d(111,010) = 2$$

وعند $v = 111$ لدينا :

$$d(000, v+u) = d(000,101) = 2$$
$$d(111, v+u) = d(111,101) = 1$$

إذن ، C تصوّب نمط الخطأ $u = 010$.

(ب) عند $v = 000$ لدينا :

$$d(000, v+u) = d(000,110) = 2$$
$$d(111, v+u) = d(111,110) = 1$$

وبما أن $v + u$ ليس أقرب إلى $v = 000$ منه إلى $v = 111$ فنرى أن C لا تصوّب نمط الخطأ $u = 110$. ▲

من الممكن الاستعانة بجدول IMLD لمعرفة أنماط الأخطاء التي يمكن تصويبها بواسطة الشفرة C. بالنظر إلى أي عمود نمط خطأ نجد أن كل نمط من أنماط الأخطاء الممكنة (أي كلمات K^n) يقع مرة واحدة في هذا العمود (إذا وقع نمط الخطأ u مرتين في العمود لكلمة شفرة واحد v فإن u تقع في صفين يقابلان كلمتين مستقبلتين مختلفتين w_1 و w_2. وبهذا يكون $u = v + w_1 = v + w_2$ وهذا مستحيل ؛ لأن $w_1 \neq w_2$). كما أن العلامة * في جدول IMLD توضع بجانب نمط الخطأ u في عمود يقابل كلمة الشفرة v إذا كانت $v + u$ أقرب إلى v منها إلى أي كلمة شفرة أخرى. وبهذا نرى أن C تصوّب نمط الخطأ u إذا وجدت العلامة * بجانب u في جميع أعمدة أنماط الأخطاء في جدول IMLD.

مثال (١,١٢,٢)

جدول IMLD للشفرة $C = \{000\,,111\}$ مبين في الجدول (١,١). توجد علامة * بجانب نمط الخطأ 010 في جميع صفوف وقوعه (الصفان 3 و 6) ولذا فإن طريقة IMLD

تستنتج صواباً أن الكلمة v هي المرسلة ومن ثم فإن C تصوّب نمط الخطأ 010. أما بالنسبة لنمط الخطأ 110 فلا توجد علامة * بجانبه في صف واحد على الأقل من صفوف وقوعه (الصف 4). ونرى أنه لو كانت 111 هي الكلمة المرسلة وأن 001 هي الكلمة المستقبلة فإن طريقة IMLD تستنتج خطأ أن الكلمة المرسلة هي 000. ولذا فإن C لا تصوّب نمط الخطأ 110. لاحظ أيضاً أن C تصوّب جميع أنماط الأخطاء 000، 100، 010، 001 الموضوع بجانبها علامة * في جميع صفوف وقوعها. وبهذا تكون C شفرة تصوّب أنماط الأخطاء من النوع 1. ▲

مثال (١,١٢,٣)

جدول IMLD للشفرة $C = \{0000, 1010, 0111\}$ مبين في الجدول (١,٢). يقع نمط الخطأ $u = 1010$ في الصفوف 1، 7، 13 والوقوع الوحيد الموضوع بجانبه علامة * هو الوقوع في الصف 13. ولذا فإن C لا تصوّب نمط الخطأ $u = 1010$. ولكن C تصوّب جميع أنماط الأخطاء 0000، 0100، 0001. ▲

مثال (١,١٢,٤)

هل الشفرة $C = \{001, 101, 110\}$ تصوّب نمط الخطأ $u = 100$ ؟

الحل

صفوف جدول IMLD التي يظهر فيها نمط الخطأ $u = 100$ مبينة في الجدول التالي.

فك التشفير	أنماط الأخطاء			الكلمات المستقبلة
v	$110+w$	$001+w$	$101+w$	w
101	011	000*	100	101
001	111	100	000*	001
110	100*	111	011	010

بالنظر إلى الجدول نجد أن الوقوع الوحيد لنمط الخطأ $u = 100$ الموضوع بجانبه * هو الوقوع في الصف الثالث. ولذا فإن C لا تصوّب نمط الخطأ $u = 100$. ▲

تمارين

(**١,١٢,٥**) لتكن $C = \{001, 101, 110\}$. هل تصوّب الشفرة C نمط الخطأ $u = 100$ ؟
ماذا عن نمط الخطأ $u = 000$ ؟

(**١,١٢,٦**) أثبت أن نمط الخطأ نفسه لا يمكن أن يقع في صفين مختلفين من جدول IMLD.

(**١,١٢,٧**) أثبت أن جميع الشفرات تصوّب نمط الخطأ صفر.

(**١,١٢,٨**) أي من أنماط الأخطاء تصوبها الشفرة $C = K^n$ ؟

من الممكن استخدام مفهوم مسافة الشفرة لتصميم اختبار لتصويب الأخطاء عوضاً عن استخدام طريقة IMLD الشّاقة أحياناً. وهذا الاختبار هو فحوى المبرهنة التالية. تذكر أن الرمز $\lfloor x \rfloor$ يعني أكبر عدد صحيح لا يزيد عن العدد الحقيقي x. فمثلاً، $\lfloor 5/2 \rfloor = 2$، $\lfloor 3 \rfloor = 3$، $\lfloor 1/2 \rfloor = 0$.

مبرهنة (١,١٢,٩)

لتكن C شفرة مسافتها d. عندئذ، C تصوّب جميع أنماط الأخطاء التي وزنها لا يزيد عن $\lfloor (d-1)/2 \rfloor$. إضافة إلى ذلك يوجد على الأقل نمط خطأ واحد وزنه $\lfloor (d-1)/2 \rfloor + 1$ لا تصوّبه الشفرة C.

البرهان

لنفرض أن u نمط خطأ حيث $wt(u) \le (d-1)/2$. وليكن $v, w \in C$ حيث $w \ne v$.
سنبرهن أن $d(v, v+u) < d(w, v+u)$. الآن

$d(w, v+u) + wt(u) = d(w, v+u) + d(v+u, v)$	(تعريف الوزن)
$\ge d(w, v)$	(متباينة المثلث)
$\ge d$	(تعريف مسافة الشفرة)
$\ge 2wt(u) + 1$	(الفرض)

إذن، $d(v,v+u)=wt(u)<wt(u)+1\leq d(w,v+u)$. وبهذا نرى أن C تصوّب نمط الخطأ u.

نفرض الآن أن $v,w\in C$ حيث $d(v,w)=d$ (لاحظ أن $wt(v+w)=d$). ولنفرض أن u هو نمط الخطأ الذي نحصل عليه من $v+w$ بتغيير عدد $d-1-\lfloor(d-1)/2\rfloor$ من الواحدات إلى أصفار. عندئذ

$$wt(u)=d-(d-1-\lfloor(d-1)/2\rfloor=1+\lfloor(d-1)/2\rfloor$$

سنبرهن الآن أن C لا تصوّب u وذلك بإثبات أن $d(w,v+u)\leq d(v,v+u)$.

ندرس الحالتين: d فردي و d زوجي.

لنفرض أولاً أن d فردي. أي أن $d=2t+1$ حيث $t\in\mathbb{Z}$. في هذه الحالة يكون $t=\lfloor(d-1)/2\rfloor$. من ذلك نرى أن:

$$\begin{aligned}
d(v,v+u)\ &=wt(u)=1+t\\
d(w,v+u)&=wt(w+v+u)=d(v+w,u)\\
&=d-(1+\lfloor(d-1)/2\rfloor)\\
&=(2t+1)-(1+t)=t
\end{aligned}$$

وبهذا نرى في هذه الحالة أن $d(w,v+u)\leq d(w,v+u)$.

أما إذا كان d زوجياً فإن $d=2t$ ويكون $\lfloor(d-1)/2\rfloor=\mathrm{t}-1$. من ذلك نجد أن:

$$\begin{aligned}
d(v,v+u)&=wt(u)=1+(t-1)=t\\
d(w,v+u)&=wt(w+v+u)=d(v+w,u)\\
&=d-(1+\lfloor(d-1)/2\rfloor)\\
&=2t-(1+(t-1)\\
&=t
\end{aligned}$$

وبهذا نستنتج أن $d(w,v+u)\leq d(v,v+u)$. وعليه نرى أن $v+u$ ليس أقرب إلى v منه إلى w ونخلص إلى أن C لا تصوّب نمط الخطأ u. ■

من الواضح، استناداً إلى المبرهنة (**١,١٢,٩**) أن الشفرة ذات المسافة d هي شفرة تصويب أنماط أخطاء من النوع $\lfloor(d-1)/2\rfloor$.

مثال (١,١٢,١٠)

مسافة الشفرة $C = \{000\,, 111\}$ هي $d = 3$. بما أن $\lfloor (d-1)/2 \rfloor = 1$ فنجد استناداً إلى المبرهنة (**١,١٢,٩**) أن C تصوّب جميع أنماط الأخطاء من الوزن 0 أو 1. وكما رأينا من المثال (**١,١٢,١**) فإن C تصوّب فعلاً أنماط الأخطاء 000، 100، 010، 001. وزن نمط الخطأ 110 يساوي $\lfloor (d-1)/2 \rfloor + 1 = 2$ وسبق وأن رأينا أن C لا تصوّب نمط الخطأ هذا. ▲

لاحظ أن المبرهنة (**١,١٢,٩**) لا تمنع شفرة C مسافتها d من تصويب أنماط أخطاء وزنها أكبر من $\lfloor (d-1)/2 \rfloor$.

مثال (١,١٢,١١)

مسافة الشفرة $C = \{001\,, 101\}$ هي $d = 1$ ووزن نمط الخطأ $u = 011$ هو 2 وهذا أكبر من $\lfloor (d-1)/2 \rfloor + 1 = 1$ ومع ذلك فالشفرة C تصوّب نمط الخطأ $u = 011$ كما هو موضّح في جزء جدول IMLD التالي.

w	$001 + w$	$101 + w$	v
010	011*	111	001
110	111	011*	101

تمارين

(**١,١٢,١٢**) لكل من الشفرات التالية:

(i) عيّن أنماط الأخطاء التي تصوّبها C. أُنشئت جداول IMLD لهذه الشفرات في التمرين (**١,٩,٧**).

(ii) عيّن أنماط الأخطاء التي تضمن المبرهنة (**١,١٢,٩**) تصويبها بواسطة C.

(أ) $C = \{101\,, 111\,, 011\}$

(ب) $C = \{000\,, 001\,, 010\,, 011\}$

(ج) $C = \{0000\,, 0001\,, 1110\}$

(د) $C = \{0000\, , 1001\, , 0110\, , 1111\}$

(هـ) $C = \{00000\, , 11111\}$

(و) $C = \{00000\, , 11100\, , 00111\, , 11011\}$

(ز) $C = \{00000\, , 11110\, , 01111\, , 10001\}$

(ح) $C = \{000000\, , 101010\, , 010101\, , 111111\}$

(**١,١٢,١٣**) استخدم طريقة المثال (**١,١٢,١١**) لتحديد فيما إذا كانت الشفرة المعطاة تصوّب أنماط الأخطاء المعطاة.

(أ) $C = \{000000\, , 100101\, , 010110\, , 001111\, ,$
$110011\, , 101010\, , 011001\, , 111100\}$

(i) $u = 001000$
(ii) $u = 000010$
(iii) $u = 100100$

(ب) $C = \{1001011\, , 0110101\, , 1110010\, , 1111111\}$

(i) $u = 0100000$
(ii) $u = 0101000$
(iii) $u = 1100000$

(**١,١٢,١٤**) لكل شفرة من شفرات التمرين (**١,١٢,١٢**)، جد نمط خطأ من الوزن $1 + \lfloor (d-1)/2 \rfloor$ لا تصوّبه الشفرة.

(**١,١٢,١٥**) لتكن C شفرة تحتوي جميع الكلمات ذات الطول 4 وذات الوزن الزوجي. عيّن أنماط الأخطاء التي تصوّبها C.

(**١,١٢,١٦**) لنفرض أن u_1 و u_2 نمطا خطأ طول كل منهما يساوي n ولنفرض أن u_1 و u_2 يتفقان على الأقل في المواقع التي تكون فيها إحداثيات u_1 تساوي 1. إذا كانت C تصوّب u_2 فأثبت أنها تصوّب u_1 أيضاً.

لاحظنا سابقاً أن احتمال وقوع أنماط الأخطاء ذوات الأوزان الصغيرة أكثر من احتمال وقوع أنماط الأخطاء ذوات الأوزان الكبيرة (المبرهنة (**١,٦,٣**)). وبناء على ذلك فعند تصميم الشفرات يجب التركيز على تصميم شفرات يكون بمقدورها تصويب أو على الأقل اكتشاف أنماط الأخطاء ذوات الأوزان الصغيرة.

الفصل الثاني

الشفرات الخطية
Linear Codes

(٢,١) الشفرات الخطية
Linear Codes

نقدم في هذا البند صنفاً عاماً من الشفرات حيث تنتمي جميع الشفرات التي سندرسها إلى هذا الصنف. وبدراستنا لهذا الصنف يكون بمقدورنا توظيف بعض المفاهيم الرياضية المهمة التي تساعدنا على حل بعض المسائل التي سبق وأن ناقشناها للشفرات التي تنتمي إلى هذا الصنف.

نقول إن الشفرة C **شفرة خطية على الحقل K (Linear Code)** إذا كانت $v + w \in C$ لكل $w, v \in C$. أي أن الشفرة الخطية هي الشفرة المغلقة تحت عملية جمع الكلمات. على سبيل المثال، الشفرة $C = \{000\,,111\}$ شفرة خطية ؛ لأن جميع المجاميع الأربعة :

$$000 + 000 = 000$$
$$000 + 111 = 111$$
$$111 + 000 = 111$$
$$111 + 111 = 000$$

تنتمي إلى الشفرة C. ولكن الشفرة $C_1 = \{000\,,001\,,101\}$ ليست خطية ؛ لأن $001,101 \in C_1$ ولكن $001 + 101 = 100 \notin C_1$.

لاحظ أنه إذا كانت C شفرة خطية وكانت $v \in C$ فإن $v + v = 0 \in C$. وبهذا نرى أن أي شفرة خطية يجب أن تحتوي الكلمة الصفرية. ولكن العكس ، غير صحيح ، فالشفرة C_1 المقدمة في الفقرة السابقة تحتوي على الكلمة الصفرية ولكنها ليست شفرة خطية.

تمارين

(**٢,١,١**) بيّن أي من الشفرات التالية هي شفرة خطية :

(أ) $C = \{101\,, 111\,, 011\}$

(ب) $C = \{000\,, 001\,, 010\,, 011\}$

(ج) $C = \{0000\,, 0001\,, 1110\}$

(د) $C = \{0000\,, 1001\,, 0110\,, 1111\}$

(هـ) $C = \{00000\,, 11111\}$

(و) $C = \{00000\,, 11100\,, 00111\,, 11011\}$

(ز) $C = \{00000\,, 11110\,, 01111\,, 10001\}$

(ح) $C = \{000000\,, 101010\,, 010101\,, 111111\}$

إحدى خصائص الشفرة الخطية التي تميزها عن الشفرات غير الخطية هي سهولة حساب مسافتها. فمسافة الشفرة الخطية هي أصغر أوزان كلماتها غير الصفرية. برهان هذه الحقيقة السهلة هو فحوى التمرين (**٢,١,٤**).

تمارين

(**٢,١,٢**) أثبت أن الشفرة $C = \{0000,1100,0011,1111\}$ خطية وأن مسافتها هي $d = 2$.

(**٢,١,٣**) جد مسافة كل من الشفرات الخطية المقدمة في التمرين (**٢,١,١**) ثم تحقق من أن ذلك يتفق مع ما وجدته في التمرين (**١,١١,١٢**).

(**٢,١,٤**) أثبت أن مسافة الشفرة الخطية تساوي أصغر أوزان كلماتها غير الصفرية.

سنرى في البنود القادمة أن سهولة حساب مسافة الشفرة الخطية ليست الميزة الوحيدة التي تجعلها أفضل من الشفرات غير الخطية، بل توجد عديد من الميزات الأخرى لهذه الشفرات حيث إن عديداً من المسائل التي يصعب معالجتها للشفرات العامة تكون معالجتها سهلة للشفرات الخطية وإليك بعض الأمثلة على ذلك:

(١) توجد خوارزمية أسهل وأسرع للتنفيذ لإيجاد MLD للشفرات الخطية من الخوارزمية المقدمة سابقاً (في الحقيقة، للشفرات الخطية التي تتمتع بخواص إضافية تكون خوارزمية فك التشفير سهلة جداً).

(٢) تشفير الشفرة الخطية أسرع ويحتاج إلى سعة تخزين أقل من الشفرات غير الخطية.

(٣) حساب الاحتمالات $\theta_p(C,v)$ مباشر للشفرات الخطية.

(٤) من السهل وصف أنماط الأخطاء التي تكتشفها الشفرة الخطية.

(٥) من السهل وصف أنماط الأخطاء التي تصوّبها الشفرة الخطية.

يُعد الجبر الخطي من أهم الموضوعات التي نحتاجها لدراسة الشفرات الخطية. ففي هذا البند وبعض البنود القادمة سنراجع بعض الحقائق الأساسية من الجبر الخطي ونحاول أن نبين أهمية ذلك لنظرية التشفير. معظم البراهين التي لا تعتمد على الضرب بعدد قياسي في K^n هي نسخة مطابقة تماماً للبراهين في $\mathbb{R}^n$ ومن ثم سنسقطها.

تذكر أن فضاء المتجهات K^n على K (يُسمى K حقل الأعداد القياسية) يتكون من مجموعة من متجهات (أو كلمات) K^n معرفاً عليها عملية الضرب بعدد قياسي وعملية جمع متجهات ويحقق الشروط العشرة التي قدمناها في البند (١,٧). نقول إن مجموعة جزئية غير خالية U من فضاء متجهات V، **فضاءً جزئياً من V (Subspace of V)** إذا كانت U مغلقة تحت عمليتي جمع المتجهات والضرب بعدد قياسي. أي أنه إذا كان $v,w \in U$ وكان a عدداً قياسياً فإن $v+w \in U$ وإن $av \in U$.

وعلى وجه الخصوص، بما أن أعداد K القياسية هي 0 و 1 فقط فتكون U فضاءً جزئياً من K^n إذا وفقط إذا كانت المجموعة الجزئية U مغلقة تحت عملية الجمع. وبهذا نرى أن الشفرة C خطية إذا وفقط إذا كانت فضاءً جزئياً من K^n. في البنود القليلة القادمة، نستخدم مفهوم الفضاءات الجزئية لتسهيل عمليتي التشفير وفك التشفير.

(٢,٢) فضاءان جزئيان مهمان
Two Important Subspaces

نقدم الآن فضائين جزئيين من فضاء المتجهات K^n وهما مثالان مهمان على الشفرات الخطية حيث سيؤديان دوراً مهماً في دراستنا المستقبلية. سنقدم التعاريف والنتائج على فضاء متجهات عام ثم نوظفها لفضاء المتجهات K^n.

نقول إن المتجه w **تركيب خطي (Linear Combination)** للمتجهات $v_1, v_2, \cdots, v_k$ إذا وجدت أعداد قياسية $a_1, a_2, \cdots, a_k$ بحيث يكون:

$$w = a_1 v_1 + a_2 v_2 + \cdots + a_k v_k$$

تُسمى جميع التركيبات الخطية لمتجهات المجموعة $S = \{v_1, v_2, \cdots, v_k\}$، **الفضاء الخطي المولّد بالمجموعة S (Linear Span of S)** ويُرمز له بالرمز $\langle S \rangle$. إذا كانت $S = \emptyset$ فنعرّف $\langle S \rangle = \{0\}$.

من المعلوم في الجبر الخطي أنه لأي مجموعة جزئية S من فضاء متجهات V يكون الفضاء الخطي المولّد الخطي $\langle S \rangle$ فضاءاً جزئياً من V ويُسمى **الفضاء الجزئي المولّد بالمجموعة S (Subspace Spanned or Generated by S)**. في حالة فضاء المتجهات K^n يوجد وصف سهل للفضاء الجزئي $\langle S \rangle$ وهو فحوى المبرهنة التالية. وبما أن $\langle S \rangle$ فضاء جزئي من K^n فنسمي $\langle S \rangle$ من الآن فصاعداً، **الشفرة الخطية المولّدة بالمجموعة S (Linear Code Generated by S)**.

مبرهنة (٢,٢,١)

لتكن $S \subseteq K^n$. تتكون الشفرة $C = \langle S \rangle$ من الكلمات التالية :

الكلمة الصفرية، جميع كلمات S، جميع مجاميع كلمتين أو أكثر من كلمات S. ■

مثال (٢,٢,٢)

إذا كانت $S = \{0100, 0011, 1100\}$ فإن كلمات الشفرة $C = \langle S \rangle$ هي :

$$0000, 0100, 1100, 0011$$
$$0100 + 0011 = 0111$$
$$0100 + 1100 = 1000$$
$$0011 + 1100 = 1111$$
$$0100 + 0011 + 1100 = 1011$$

وبهذا يكون :

$$C = \langle S \rangle = \{0000, 0100, 0011, 1100, 0111, 1000, 1111, 1011\}$$ ▲

تمرين

(**٢,٢,٣**) جد عناصر الشفرة الخطية $\langle S \rangle$ لكل من المجموعات S التالية :

(أ) $S = \{010, 011, 111\}$

(ب) $S = \{1010, 0101, 1111\}$

(ج) $S = \{0101, 1010, 1100\}$

(د) $S = \{1000, 0100, 0010, 0001\}$

(هـ) $S = \{11000, 01111, 11110, 01010\}$

(و) $S = \{10101, 01010, 11111, 00011, 10110\}$.

إذا كان $v = (a_1, a_2, \cdots, a_n), w = (b_1, b_2, \cdots, b_n) \in K^n$ فنُعرّف **الضرب القياسي أو الضرب النقطي (Scalar or Dot Product)** $v \cdot w$ للمتجهين v و w على النحو التالي :

$$v \cdot w = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

لاحظ أن $v \cdot w$ عدد قياسي. على سبيل المثال، في الفضاء K^5 لدينا:

$$\begin{aligned} 11001 \cdot 01101 &= 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 \\ &= 0 + 1 + 0 + 0 + 1 \\ &= 0 \end{aligned}$$

تمارين

(**٢,٢,٤**) جد أمثلة في الفضاء K^5 للقاعدتين التاليتين:

(أ) $u \cdot (v + w) = u \cdot v + u \cdot w$

(ب) $a(v \cdot w) = (av) \cdot w = v \cdot (aw)$

(**٢,٢,٥**) أثبت صواب القاعدتين المقدمتين في التمرين (**٢,٢,٤**) في الفضاء K^n.

نقول إن المتجهين v و w **متعامدان (Orthogonal)** إذا كان $v \cdot w = 0$. المثال المقدم في الفقرة أعلى الصفحة يُبين أن المتجهين $v = 11001$ و $w = 01101$ متعامدان في الفضاء K^5. إذا كانت S مجموعة جزئية من K^n وكان $v \in K^n$ فنقول إن v **عمودي على المجموعة S (Orthogonal to the Set S)** إذا كان $v \cdot w = 0$ لكل $w \in S$. أي أن v عمودي على جميع متجهات S. يُرمز لمجموعة جميع المتجهات العمودية على S بالرمز $S^{\perp}$ وتُسمى **المتمم العمودي على S (Orthogonal Complement of S)**.

نعلم من الجبر الخطي أنه إذا كانت S مجموعة جزئية من فضاء متجهات V فإن المتمم العمودي $S^{\perp}$ فضاء جزئي من V(١). إذا كانت $C = \langle S \rangle$ في الفضاء K^n فنكتب $C^{\perp} = S^{\perp}$ ونقول إن $C^{\perp}$ هي **الشفرة الثنوية للشفرة C (The Dual Code of C)**.

---

(١) المترجمان: بما أن $\mathbf{0} \cdot w = 0$ لكل $w \epsilon S$ فنجد أن $\mathbf{0} \epsilon S$.

وإذا كان $w, u \epsilon S^{\perp}$ و $\alpha \epsilon K$ فعندئذ لكل $v \epsilon S$ لدينا:

$$\begin{aligned} v \cdot (w + u) &= v \cdot w + v \cdot u = 0 + 0 \\ (kv) \cdot w &= k(v \cdot w) = k \cdot 0 = 0 \end{aligned}$$

وبهذا يكون $S^{\perp}$ فضاءاً جزئياً من V.

مثال (٢,٢,٦)

إذا كانت $S = \{0100\,,0101\}$ فاحسب الشفرة الثنوية $C^{\perp} = S^{\perp}$.

الحل

المطلوب إيجاد جميع الكلمات $v = (x, y, z, w)$ في K^4 التي تحقق المعادلتين:

$$v \cdot 0100 = 0$$
$$v \cdot 0101 = 0$$

وبحساب الضرب القياسي نجد أن:

$$y = 0$$
$$y + w = 0$$

وبهذا نرى أن $y = w = 0$. وأما كل من x و z فتأخذ أياً من القيمتين 0 أو 1 (أي عنصر من عناصر K). وبإيجاد جميع الخيارات الممكنة للمتجه v نحصل على $C^{\perp} = S^{\perp} = \{0000\,,0010\,,1000\,,1010\}$. ▲

تمارين

(**٢,٢,٧**) عيّن الشفرة الثنوية $C^{\perp}$ لكل من الشفرات $C = \langle S \rangle$ المبينة في التمرين (**٢,٢,٣**).

(**٢,٢,٨**) جد مثالاً لكلمة غير صفرية v بحيث يكون $v \cdot v = 0$. ماذا يمكن القول عن أوزان مثل هذه الكلمات ؟

(**٢,٢,٩**) إذا كانت S مجموعة جزئية من فضاء المتجهات V فأثبت أن $\langle S \rangle = (S^{\perp})^{\perp}$. استخدم المثال (**٢,٢,٦**) لإعطاء مثال لهذه الحقيقة في الفضاء K^4.

(**٢,٢,١٠**) أثبت أن $\langle S \rangle \subseteq (S^{\perp})^{\perp}$ (في الحقيقة، $(S^{\perp})^{\perp} = \langle S \rangle$) وللشفرات الخطية C هذا يعني أن $(C^{\perp})^{\perp} = C$.

(٢,٣) الاستقلال والأساس والبُعد

Independence, Basis, Dimension

نُقدم مراجعة عامة لعدة مفاهيم من الجبر الخطي ثم نوضح كيفية توظيف هذه المفاهيم للشفرات الخطية. الهدف الرئيس هو إيجاد طريقة فعّالة لوصف الشفرة الخطية

دون اللجوء إلى سرد جميع كلماتها. نقول إن مجموعة من المتجهات $S = \{v_1, v_2, \cdots, v_k\}$ **مرتبطة خطياً (Linearly Dependent)** إذا وجدت أعداد قياسية $a_1, a_2, \cdots, a_k$ ليست كلها أصفاراً بحيث يتحقق:

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$$

وإذا لم تكن S مرتبطة خطياً فنقول إنها **مُستقلة خطياً (Linearly Independent)**. أي أن S مُستقلة خطياً إذا تحقق ما يلي لكل أعداد قياسية $a_1, a_2, \cdots, a_k$

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0 \Rightarrow a_1 = a_2 = \cdots = a_k = 0$$

لاختبار فيما إذا كانت مجموعة S مُستقلة خطياً نقوم بكتابة المعادلة $a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$. فإذا كان حل هذه المعادلة هو الحل التافه (أي أن $a_i = 0$ لكل $i = 1,2, \cdots, k$) فتكون S مُستقلة خطياً. أما إذا وجد على الأقل حل a_i غير صفري فتكون S مرتبطة خطياً.

مثال (٢,٣,١)

أثبت أن $S = \{1001 , 1101 , 1011\}$ مجموعة جزئية مُستقلة خطياً في K^4.

الحل

لنفرض أن a ، b ، c أعداد قياسية (0 أو 1) حيث:

$$a(1001) + b(1101) + c(1011) = 0000$$

بمقارنة إحداثيات الطرفين نحصل على نظام المعادلات

$$a + b + c = 0$$
$$b = 0$$
$$c = 0$$

وبحل هذا النظام نجد أن $a = b = c = 0$. إذن، S مُستقلة خطياً. ▲

مثال (٢,٣,٢)

أثبت أن $S = \{110 , 011 , 101 , 111\}$ مرتبطة خطياً في K^3.

الحل

نفرض أن a ، b ، c ، d أعداد قياسية حيث:

$$a(110) + b(011) + c(101) + d(111) = 000$$

بمقارنة إحداثيات الطرفين نحصل على نظام المعادلات:

$$a + c + d = 0$$
$$a + b + d = 0$$
$$b + c + d = 0$$

وبحل هذا النظام نجد أن $d = 0$ وأن $a = b = c$. وباختيار $a = b = c = 1$ نستنتج أن S مرتبطة خطياً. ▲

من حقائق الجبر الخطي أنه إذا كانت $S \neq \{0\}$ مجموعة من المتجهات فتوجد مجموعة جزئية S' من S مُستقلة خطياً حيث تحتوي S' أي مجموعة جزئية أخرى من S ومُستقلة خطياً (أي أن S' أكبر مجموعة جزئية من S مُستقلة خطياً). المثال التالي يبين كيفية إيجاد مثل هذه المجموعة S'.

مثال (٢,٣,٣)

بيّنا في المثال (**٢,٣,٢**) أن المجموعة $S = \{110, 011, 101, 111\}$ مرتبطة خطياً حيث وجدنا:

$$1(110) + 1(011) + 1(101) + 0(111) = 000$$

وبهذا نستطيع كتابة 101 كتركيب خطي لكلمات S الأخرى:

$$101 = 1(110) + 1(011) + 0(111)$$

إذا اعتبرنا أن ترتيب كلمات S هو الترتيب المعطى فنرى أن 101 هي أول كلمة يمكن كتابتها كتركيب خطي لكلمات S السابقة لها وهي 110 ، 011. بحذف هذه الكلمة من S نحصل على مجموعة جديدة $S' = \{110, 011, 111\}$. إذا كانت S' مُستقلة خطياً نتوقف وتكون S' هي المجموعة الجزئية المستقلة خطياً من S المنشودة. أما إذا كانت S'

مرتبطة خطياً فنقوم بحذف أول كلمة يمكن كتابتها كترتيب خطي للكلمات السابقة لها لنحصل على مجموعة جديدة S''. وهكذا إلى أن نحصل على مجموعة مُستقلة خطياً. وعند ذلك تكون هذه أكبر مجموعة جزئية من S مُستقلة خطياً. هذه المجموعة في مثالنا هذا هي S'. ▲

تمرين

(**٢,٣,٤**) بيّن أي من المجموعات التالية مُستقلة خطياً. وإذا كانت المجموعة مرتبطة خطياً فجد أكبر مجموعة جزئية من S مُستقلة خطياً.

(أ) $S = \{1101, 1110, 1011\}$

(ب) $S = \{101, 011, 110, 010\}$

(ج) $S = \{1101, 0111, 1100, 0011\}$

(د) $S = \{1000, 0100, 0010, 0001\}$

(هـ) $S = \{1000, 1100, 1110, 1111\}$

(و) $S = \{1100, 1010, 1001, 0101\}$

(ز) $S = \{0110, 1010, 1100, 0011, 1111\}$

(ح) $S = \{111000, 000111, 101010, 010101\}$

(ط) $S = \{00000000, 10101010, 01010101, 11111111\}$.

لاحظ أن المجموعة S في التمرين (**٢,٣,٤**) (ط) مرتبطة خطياً ولاحظ أيضاً أنها تحتوي الكلمة الصفرية. في الحقيقة أي مجموعة من المتجهات التي تحتوي المتجه الصفري هي مرتبطة خطياً.

نقول عن مجموعة جزئية غير خالية B من فضاء متجهات V إنها **أساس (Basis)** للفضاء V إذا حققت الشرطين التاليين :

(١) B تولّد V (أي أن $\langle B\rangle = V$).

(٢) B مُستقلة خطياً.

لاحظ أن أي مجموعة مُستقلة خطياً B هي أساس للفضاء $\langle B\rangle$. وبما أن أي مجموعة S من المتجهات المرتبطة خطياً وغير الصفرية تحتوي على أكبر مجموعة جزئية مُستقلة خطياً B، فنستطيع أن نحصل على أساس B كمجموعة جزئية من S للفضاء $\langle S\rangle$. إذا كانت $S=\{0\}$ فنقول في هذه الحالة أن أساس S هو المجموعة الخالية $\emptyset$.

مثال (٢,٣,٥)

وجدنا في المثال (**٢,٣,١**) أن المجموعة $S=\{1001\,,1101\,,1011\}$ مُستقلة خطياً. وبهذا تكون S أساساً للشفرة $C=\langle S\rangle=\{0000,\ 1001,\ 1101, 1011,\ 0100\ ,\ 0010\ ,$ $0110\ ,\ 1111\}$ التي هي فضاء جزئي من K^4. ▲

مثال (٢,٣,٦)

وجدنا في المثال (**٢,٣,٢**) أن المجموعة $S=\{110\,,011\,,101\,,111\}$ مُرتبطة خطياً. وفي المثال (**٢,٣,٣**) وجدنا أن $B=S'=\{110\,,011\,,111\}$ هي أكبر مجموعة جزئية مُستقلة خطياً من S. وبهذا تكون B أساساً للشفرة $C=\langle S\rangle$. ▲

في المثالين السابقين بيّنا كيفية إيجاد أساس للشفرة $C=\langle S\rangle$ المولدة بمجموعة جزئية غير خالية S من K^n. لإيجاد أساس للفضاء الثنوي $C^\perp$ نقوم بإيجاد أكبر مجموعة جزئية مُستقلة خطياً من $C^\perp$ بالطريقة المبينة في المثال (**٢,٣,٣**).

تمرين

(**٢,٣,٧**) جد أساساً B للشفرة $C=\langle S\rangle$ لكل مجموعة من المجموعات المبينة في التمرين (**٢,٢,٣**) ثم جد أساساً $B^\perp$ للشفرة الثنوية $C^\perp$.

وجدنا في المثال (**٢,٣,٦**) أن المجموعة الجزئية $B=\{110\,,011\,,111\}$ هي أكبر مجموعة جزئية مُستقلة خطياً من المجموعة $S=\{110\,,011\,,101\,,111\}$. المجموعة B هذه ليست وحيدة فالمجموعة $B_1=\{110\,,101\,,111\}$ هي أيضاً أكبر مجموعة جزئية مُستقلة خطياً من S ومن ثم فهي أيضاً أساس للشفرة $C=\langle S\rangle$.

في العموم يكون لفضاء متجهات V عدد كبير من الأساسات ولكن جميع هذه الأساسات تحتوي على العدد نفسه من العناصر. يُسمى هذا العدد **بُعد فضاء المتجهات (Dimension of the Vector Space)** ويُرمز له بالرمز $dimV$. بُعد الفضاء K^n يساوي n ؛ لأن جميع الكلمات ذوات الطول n والوزن 1 أساس للفضاء K^n. ومن جهة أخرى أساس الفضاء الصفري $\{0\}$ هو $\emptyset$ ومن ثم فبُعده 0.

تمرين

(٢,٣,٨) جد بُعد كل من الشفرات $C = \langle S \rangle$ والشفرات الثنوية $C^\perp$ المقدمة في التمرين **(٢,٢,٣)** (انظر أيضاً التمرين **(٢,٢,٧)**).

يُزودنا أساس الشفرة الخطية بطريقة فعالة لوصف الشفرة؛ لأنه إذا كان $\{v_1, v_2, \cdots, v_k\}$ أساساً لأي فضاء متجهات V وكان $w \in V$ فيمكن كتابة w بطريقة وحيدة كتركيب خطي لعناصر الأساس $v_1, v_2, \cdots, v_k$. أي يمكن إيجاد أعداد قياسية وحيدة $a_1, a_2, \cdots, a_k$ بحيث يكون $w = a_1v_1 + a_2v_2 + \cdots + a_kv_k$.

مثال (٢,٣,٩)

أكتب $w = 011$ كتركيب خطي وحيد لكلمات الأساس $\{110, 001, 100\}$ للفضاء K^3.

الحل

سنجد أعداداً قياسياً a ، b ، c بحيث يكون:

$$a(110) + b(001) + c(100) = 011$$

وبمقارنة طرفي المعادلة نحصل على النظام:

$$a + c = 0$$
$$a = 1$$
$$b = 1$$

وبهذا نرى أن $a = b = c = 1$ ويكون:

$$011 = 1(110) + 1(001) + 1(100).$$ ▲

تمرين

(**٢,٣,١٠**) اكتب كلاً من كلمات K^4 التالية كتركيب خطي وحيد لكلمات الأساس $\{1000, 1100, 1110, 1111\}$.

(أ) 0011 (ب) 1010 (ج) 0111

(د) 0001 (هـ) 0000

وحقيقة أخرى مهمة عن فضاءات المتجهات هي أن أي مجموعة جزئية مُستقلة خطياً من فضاء متجهات تكون محتواة في أساس لهذا الفضاء. والمثال التالي يبيّن لنا كيفية إنجاز ذلك.

مثال (٢,٣,١١)

المجموعة الجزئية $S = \{110, 001\}$ مُستقلة خطياً في الفضاء K^3. سنقوم بتوسيع S إلى أساس للفضاء K^3 على النحو التالي: نضيف أولاً أساساً معلوماً للفضاء K^3 وليكن $\{100, 010, 001\}$ إلى المجموعة S وبهذا نحصل على مجموعة جديدة هي $S_1 = \{110, 001, 100, 010, 001\}$. الآن نستخدم الطريقة المتبعة في المثال (**٢,٣,٣**) لإيجاد أساس للفضاء K^3 كمجموعة جزئية من S_1. ويكون هو الأساس المنشود. ▲

تمرين

(**٢,٣,١٢**) (أ) عيّن أساساً للفضاء K^4 يحتوي المجموعة $\{1001, 1111\}$.

(ب) وسّع المجموعة $\{101010, 010101\}$ إلى أساس للفضاء K^6.

مبرهنة (٢,٣,١٣)

عدد كلمات شفرة خطية بُعدها k يساوي 2^k.

البرهان

إذا كانت C شفرة خطية بُعدها k وكان $\{v_1, v_2, \cdots, v_k\}$ أساساً للشفرة C فمن الممكن كتابة أي كلمة $w \in C$ على الصورة:

$$w = a_1 v_1 + a_2 v_2 + \cdots + a_k v_k$$

حيث $a_1, a_2, \cdots, a_k$ أعداد وحيدة في K. وبما أن $a_i = 0$ أو $a_i = 1$ لكل $i = 1,2,\cdots,k$ فيوجد 2^k من الخيارات المختلفة للأعداد $a_1, a_2, \cdots, a_k$ وبهذا نرى أن عدد كلمات C يساوي 2^k. ■

ويمكن برهان المبرهنة التالية باستخدام حقائق بدائية من نظرية أنظمة المعادلات الخطية.

مبرهنة (٢,٣,١٤)

لتكن $C = \langle S \rangle$ شفرة خطية مولّدة بالمجموعة الجزئية S من K^n. عندئذ:

$$dimC + dimC^{\perp} = n$$

تمارين

(**٢,٣,١٥**) تحقق من صواب المبرهنة (**٢,٣,١٤**) باستخدام إجابات التمرين (**٢,٣,٨**).

(**٢,٣,١٦**) افرض أن S مجموعة جزئية من K^7 وأن $C = \langle S \rangle$ وافرض أن بُعد $C^{\perp}$ يساوي 3.

(أ) جد بُعد $C = \langle S \rangle$.

(ب) جد عدد كلمات C.

(**٢,٣,١٧**) افرض أن S مجموعة جزئية من K^8 وافرض أن $\{11110000, 00001111, 10000001\}$ أساس للشفرة الثنوية $C^{\perp}$. جد عدد كلمات $C = \langle S \rangle$.

(**٢,٣,١٨**) المبرهنة (**٢,٣,١٤**) صحيحة أيضاً للفضاء $\mathbb{R}^n$ حيث كل متجه ينتمي إلى $\mathbb{R}^n$ يكتب بطريقة وحيدة كمجموع متجهين أحدهما ينتمي إلى $\langle S \rangle$ والآخر ينتمي إلى $S^{\perp}$ حيث $\langle S \rangle \cap S^{\perp} = \{0\}$. (فمثلاً في $\mathbb{R}^3$، خذ $\langle S \rangle$ المستوى xy و $S^{\perp}$ محور z). استخدم $S = \{000, 101\}$ لإثبات عدم صواب ذلك في الفضاء K^n.

النتيجة الأخيرة في هذا البند تتعلق بعدد الأساسات المختلفة للشفرة الخطية حيث إن عدد أساسات أي فضاء جزئي من $\mathbb{R}^n$ هو عدد غير منته ولكن هذا العدد منته للفضاءات الجزئية من K^n وهذا ما تزودنا به المبرهنة التالية.

مبرهنة (٢,٣,١٩)

إذا كان بُعد الشفرة الخطية يساوي k فإن عدد أساساتها المختلفة يساوي:

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k-2^i) \quad .$$

مثال (٢,٣,٢٠)

بُعد الشفرة الخطية K^4 يساوي 4. وبهذا نجد أن عدد أساسات K^4 المختلفة يساوي:

$$\frac{1}{4!}\prod_{i=0}^{3}(2^4-2^i)=\frac{1}{4!}(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)=840$$

لاحظ أن أي فضاء جزئي من K^n حيث $n\geq 4$ وحيث بُعده يساوي 4 يكون عدد أساساته المختلفة يساوي 840. ▲

تمارين

(**٢,٣,٢١**) ليكن b_n عدد أساسات K^n المختلفة. تحقق من صواب أعداد الجدول التالي:

n	1	2	3	4	5	6
b_n	1	3	28	840	83328	27998208

(**٢,٣,٢٢**) جد جميع أساسات كل من K^2 و K^3.

(**٢,٣,٢٣**) جد عدد الأساسات المختلفة لكل من الشفرات $C=\langle S\rangle$ حيث:

(أ) $S=\{001\,,011\,,111\}$

(ب) $S=\{1010\,,0101\,,1111\}$

(ج) $S=\{0101\,,1010\,,1100\}$

(د) $S = \{1000, 0100, 0010, 0001\}$

(هـ) $S = \{11000, 01111, 11110, 01010\}$

(و) $S = \{10101, 01010, 11111, 00011, 10110\}$.

(٢,٤) المصفوفات
Matrices

المصفوفة من الدرجة $m \times n$ هي مستطيل من الأعداد القياسية عدد **صفوفه (Rows)** يساوي m وعدد **أعمدته (Columns)** يساوي n. سنفترض أن القارئ على دراية بجبر المصفوفات على الأعداد الحقيقية. سنراجع في هذا البند المفاهيم البدائية من نظرية المصفوفات التي نحتاجها لدراسة نظرية التشفير.

إذا كانت A مصفوفة من الدرجة $m \times n$ وكانت B مصفوفة من الدرجة $n \times p$ فإن حاصل الضرب AB هو مصفوفة من الدرجة $m \times p$ حيث عنصرها في الموقع ij (أي في الصف i والعمود j) هو الضرب القياسي للصف i من المصفوفة A مع العمود j من المصفوفة B. على سبيل المثال:

$$\begin{bmatrix} 1011 \\ 0101 \end{bmatrix} \begin{bmatrix} 101 \\ 011 \\ 101 \\ 100 \end{bmatrix} = \begin{bmatrix} 100 \\ 111 \end{bmatrix}$$

لاحظ أن عدد أعمدة المصفوفة الأولى (التي على اليسار) يجب أن يساوي عدد صفوف المصفوفة الثانية (التي على اليمين) لكي يكون الضرب معرفاً.

تمرين

(**٢,٤,١**) جد حاصل ضرب كل زوج من المصفوفات التالية كلما أمكن ذلك.

$$A = \begin{bmatrix} 11011 \\ 00101 \\ 11011 \end{bmatrix}, B = \begin{bmatrix} 0101 \\ 1001 \\ 1100 \end{bmatrix}, C = \begin{bmatrix} 110110 \\ 011011 \\ 101101 \\ 101011 \end{bmatrix}, D = \begin{bmatrix} 1111 \\ 0101 \\ 1010 \\ 1101 \end{bmatrix}$$

تبقى القواعد الجبرية المعتادة للمصفوفات على الأعداد الحقيقية صحيحة على المجموعة K. **المصفوفة الصفرية (Zero Matrix)** من الدرجة $m \times n$ هي مصفوفة من الدرجة $m \times n$ جميع عناصرها أصفار. المصفوفة المربعة I من الدرجة $n \times n$ التي تكون عناصر قطرها الرئيس $(i = j)$ تساوي 1 والعناصر الأخرى تساوي 0 هي **المصفوفة المحايدة (Identity Matrix)** من الدرجة $n \times n$ وتحقق $AI = A$ و $IA = A$.

التمارين الثلاثة التالية تتناول ثلاث قواعد جبرية غير محققة للمصفوفات على K.

تمارين

(**٢,٤,٢**) جد مصفوفتين A و B من الدرجة 2×2 على K بحيث يكون $AB \neq BA$.

(**٢,٤,٣**) جد مصفوفتين A و B غير صفريتين من الدرجة 2×2 على K بحيث يكون $AB = 0$.

(**٢,٤,٤**) جد ثلاث مصفوفات A و B و C من الدرجة 2×2 على K بحيث يكون $AB = AC$ ولكن $B \neq C$.

يوجد نوعان من **العمليات الصفية الأولية (Elementary Row Operations)** التي تُجرى على مصفوفات معرفة على K هما:

(١) تبديل صفين.

(٢) استبدال صف بحاصل جمعه مع صف آخر.

نقول إن مصفوفتين **متكافئتين صفياً (Row Equivalent)** إذا استطعنا الحصول على إحداهما من الأخرى بإجراء متتالية منتهية من العمليات الصفية الأولية. ونقول إن العدد 1 في مصفوفة M على K هو **عنصر متقدم (Leading Element)** إذا لم يكن هناك 1 على يساره في الصف الواقع فيه. كما يُسمى عمود من M **عموداً متقدماً (Leading Column)** إذا احتوى على 1 متقدم. ونقول إن مصفوفة M هي على **صيغة درجية صفية (Row Echelon Form)** أو اختصاراً على صيغة REF إذا كانت جميع

صفوف M الصفرية (إن وجدت) واقعة أسفل المصفوفة وكان كل عنصر 1 متقدم يقع على يمين العنصر 1 المتقدم في الصفوف الأعلى. وأخيراً نقول إن مصفوفة M على **صيغة درجية صفية مختزلة (Reduced Row Echelon Form)** أو اختصاراً على صيغة RREF إذا كانت على صيغة REF وكل من أعمدتها المتقدمة يحتوي على العدد 1 في صف واحد فقط وجميع الأعداد الأخرى في ذلك العمود أصفاراً.

من الممكن وضع أي مصفوفة معرفة على K على صيغة REF أو RREF بإجراء متتالية منتهية من العمليات الصفية الأولية. وبهذا نرى أن أي مصفوفة تكافئ صفياً مصفوفة على صيغة REF أو RREF. الصيغة RREF لمصفوفة ما وحيدة ولكن من الممكن أن يكون لها العديد من صيغ REF.

مثال (٢,٤,٥)

عيّن صيغة RREF للمصفوفة M المبينة بإجراء عمليات صفية أولية.

الحل

$$M = \begin{bmatrix}1011\\1010\\1101\end{bmatrix} \rightarrow \begin{bmatrix}1011\\0001\\0110\end{bmatrix}$$ (اضافة الصف ١ إلى الصفين ٢ و ٣)

$$\rightarrow \begin{bmatrix}1011\\0110\\0001\end{bmatrix}$$ (تبديل الصفين 2 و 3)

$$\rightarrow \begin{bmatrix}1010\\0110\\0001\end{bmatrix}$$ (إضافة الصف ٣ إلى الصف 1) ▲

تمرين

(٢,٤,٦) جد صيغة RREF لكل من المصفوفات الأربع المقدمة في التمرين **(٢,٤,١)**.

منقول مصفوفة (Transpose of a Matrix) A من الدرجة $m \times n$ هي مصفوفة A^T من الدرجة $n \times m$ حيث العمود i من A هو الصف i من A^T. فمثلاً، منقول $A = \begin{bmatrix} 1011 \\ 0000 \\ 0111 \end{bmatrix}$ هو $A^T = \begin{bmatrix} 100 \\ 001 \\ 101 \\ 100 \end{bmatrix}$. سنحتاج إلى الحقيقتين التاليتين عن منقول المصفوفات:

$(A^T)^T = A$ و $(AB)^T = B^T A^T$.

(٢,٥) أساسات لكل من $C = \langle S \rangle$ و $C^{\perp}$

Bases for $C = \langle S \rangle$ & $C^{\perp}$

نقدم في هذا البند خوارزميات لإيجاد أساسات للشفرة الخطية وثنويتها وستساعدنا هذه الخوارزميات كثيراً في دراسة الشفرات الخطية.

لنفرض أن S مجموعة جزئية غير خالية من K^n. الخوارزميتان التاليتان تقدمان لنا أساساً للشفرة الخطية $C = \langle S \rangle$ المولّدة بالمجموعة S.

خوارزمية (٢,٥,١) [إيجاد أساس للشفرة C]

لتكن المصفوفة A هي المصفوفة التي صفوفها كلمات S. جد REF (أو RREF) للمصفوفة A بإجراء عمليات صفية أولية. عندئذ، الصفوف غير الصفرية في الصيغة REF هي أساس للشفرة $C = \langle S \rangle$.

لتبرير صواب الخوارزمية لاحظ أن صفوف A تولّد C وأن العمليات الصفية الأولية إما أنها تبدل كلمات أو تقوم باحلال كلمة (صف) مكان كلمة أخرى تنتمي إلى C ونتيجة لذلك نحصل على مجموعة جديدة من كلمات الشفرة التي لا زالت تولّد C. ومن الواضح أيضاً أن الصفوف غير الصفرية من صيغة REF مُستقلة خطياً.

مثال (٢,٥,٢)

عيّن أساساً للشفرة الخطية $C = \langle S \rangle$ حيث $S = \{11101, 10110, 01011, 11010\}$.

الحل

بوضع كلمات S كصفوف المصفوفة A وإيجاد صيغة REF نحصل على :

$$A=\begin{bmatrix}11101\\10110\\01011\\11010\end{bmatrix}\rightarrow\begin{bmatrix}11101\\01011\\01011\\00111\end{bmatrix}\rightarrow\begin{bmatrix}11101\\01011\\00111\\00000\end{bmatrix}$$

وبهذا نرى استناداً إلى الخوارزمية (**٢,٥,١**) أن $\{11101\,,01011\,,00111\}$ أساس للشفرة الخطية $C=\langle S\rangle$. وصيغة REF أخرى للمصفوفة A هي :

$$\begin{bmatrix}11101\\01101\\00111\\00000\end{bmatrix}$$

ويكون $\{11101\,,01101\,,00111\}$ أساساً آخر للشفرة الخطية $C=\langle S\rangle$. ▲

ملحوظة

لاحظ أن الأساس الذي نحصل عليه من الخوارزمية (**٢,٥,١**) ليس وحيداً كما هو موضح في المثال (**٢,٥,٢**). كما أن الأساس ليس بالضرورة أن يكون مجموعة جزئية من S.

تمرين

(**٢,٥,٣**) استخدم الخوارزمية (**٢,٥,١**) لإيجاد أساس للشفرة الخطية $C=\langle S\rangle$ لكل من المجموعات S التالية.

(أ) $S=\{010\,,011\,,111\}$

(ب) $S=\{1010\,,0101\,,1111\}$

(ج) $S=\{0101\,,1010\,,1100\}$

(د) $S=\{1000\,,0100\,,0010\,,0001\}$

(هـ) $S=\{11000\,,01111\,,11110\,,01010\}$

(و) $S=\{10101\,,01010\,,11111\,,00011\,,10110\}$

(ز) $S = \{0110, 1010, 1100, 0011, 1111\}$

(ح) $S = \{111000, 000111, 101010, 010101\}$

(ط) $S = \{00000000, 10101010, 01010101, 11111111\}$.

خوارزمية (٢,٥,٤) [إيجاد أساس للشفرة C]

ضع كلمات S كأعمدة لمصفوفة A. استخدم العمليات الصفية الأولية على المصفوفة A لإيجاد صيغة REF (أو RREF). عيّن الأعمدة المتقدمة في صيغة REF. عندئذ، أعمدة المصفوفة A التي تقابل الأعمدة في صيغة REF هي أساس للشفرة الخطية $C = \langle S \rangle$.

من حقائق الجبر الخطي أنه إذا كانت أعمدة مصفوفة A مُستقلة خطياً فإن أعمدة المصفوفة التي نحصل عليها بعد إجراء عدد من العمليات الصفية الأولية على A، تكون أيضاً مُستقلة خطياً. ومن السهل إثبات أن الأعمدة المتقدمة لمصفوفة على صيغة REF مُستقلة خطياً.

مثال (٢,٥,٥)

استخدم الخوارزمية (**٢,٥,٤**) لإيجاد أساس للشفرة الخطية $C = \langle S \rangle$ حيث S هي كما في المثال (**٢,٥,٢**).

الحل

بوضع كلمات S كأعمدة لمصفوفة A وإجراء عمليات صفية أولية لإيجاد صيغة REF نحصل على:

$$A = \begin{bmatrix} 1101 \\ 1011 \\ 1100 \\ 0111 \\ 1010 \end{bmatrix} \to \begin{bmatrix} 1101 \\ 0110 \\ 0001 \\ 0111 \\ 0111 \end{bmatrix} \to \begin{bmatrix} 1101 \\ 0110 \\ 0001 \\ 0000 \\ 0000 \end{bmatrix}$$

الأعمدة المتقدمة في صيغة REF هي 1، 2، 4 وبهذا تكون كلمات الأعمدة 1، 2، 4 من المصفوفة A وهي $\{11101, 10110, 11010\}$ أساساً للشفرة الخطية $C = \langle S \rangle$. ▲

ملحوظة

لاحظ أن الأساس الذي نحصل عليه من الخوارزمية (**٢,٥,٤**) للشفرة $C = \langle S \rangle$ هو مجموعة جزئية من المجموعة S.

تمرين

(**٢,٥,٦**) استخدم الخوارزمية (**٢,٥,٤**) لإيجاد أساس للشفرة $C = \langle S \rangle$ لكل مجموعة S من مجموعات التمرين (**٢,٥,٣**) ثم قارن إجاباتك.

الخوارزمية التالية تُزودنا بأساس للشفرة الثنوية $C^{\perp}$ والتي سنستخدمها في العديد من المواقع في هذا الكتاب. تقدم لنا هذه الخوارزمية أيضاً أساساً للشفرة C؛ لأن الخوارزمية (**٢,٥,١**) هي جزء منها.

خوارزمية (٢,٥,٧) [إيجاد أساس للشفرة $C^{\perp}$]

(١) ضع كلمات S كصفوف مصفوفة A.

(٢) استخدم العمليات الصفية الأولية لإيجاد صيغة RREF للمصفوفة A.

(٣) افرض أن G هي المصفوفة من الدرجة $k \times n$ المكوّنة من صفوف RREF غير الصفرية.

(٤) افرض أن X هي المصفوفة من الدرجة $k \times (n-k)$ التي نحصل عليها من G بحذف أعمدة G المتقدمة.

(٥) افرض أن H هي المصفوفة من الدرجة $n \times (n-k)$ التي نحصل عليها كالتالي:

(أ) صفوف H المقابلة لأعمدة G المتقدمة هي صفوف X (مع المحافظة على الترتيب نفسه). عدد هذه الصفوف يساوي k.

(ب) ضع في بقية صفوف H (وعددها $n-k$) المصفوفة المحايدة I من الدرجة $(n-k) \times (n-k)$ (مع المحافظة على الترتيب نفسه).

(٦) أعمدة H هي أساس للشفرة $C^{\perp}$.

لاحظ أن أعمدة H (عددها $n-k$) مُستقلة خطياً وأن:

$$dimC^{\perp} = n - dimC = n - k$$

كما أن $GH = X + X = 0$ (بعد القيام بالتبديل اللازم لأعمدة G وصفوف H).

وهذا يبرر صحة الخوارزمية.

الوصف التالي للخوارزمية (**٢,٥,٧**) يساعد على تذكرها. لاحظ أن عدد أعمدة G المتقدمة يساوي k. بتبديل أعمدة G بحيث تصبح أعمدتها المتقدمة في البداية وبهذا تكون بقية أعمدتها هي المصفوفة X. نعيد الآن تسمية المصفوفة G ونسميها G'. أي أن $G' = [I_k|X]$.

بهذا نرى أن خطوات الخوارزمية (**٢,٥,٧**) تأخذ المسار التالي: $(I_k|X)$

(١) $A \to \begin{bmatrix} G \\ 0 \end{bmatrix}$ (RREF).

(٢) $G' = [I_k|X]$ (بعد تبديل أعمدة G).

(٣) $H' = \begin{bmatrix} X \\ I_{n-k} \end{bmatrix}$.

(٤) H هي المصفوفة التي نحصل عليها من H' بتبديل صفوف H' (هذا التبديل هو عكس التبديل الذي استخدمناه لتبديل أعمدة G).

مثال (٢,٥,٨)

استخدم الخوارزمية (**٢,٥,٧**) لإيجاد أساس للشفرة الثنوية $C^{\perp}$ حيث S هي كما في المثال (**٢,٥,٢**).

الحل

$$A = \begin{bmatrix} 11101 \\ 10110 \\ 01011 \\ 11010 \end{bmatrix} \to \begin{bmatrix} 11101 \\ 01011 \\ 00111 \\ 00000 \end{bmatrix} \to \begin{bmatrix} 11010 \\ 01011 \\ 00111 \\ 00000 \end{bmatrix} \to \begin{bmatrix} 10001 \\ 01011 \\ 00111 \\ 00000 \end{bmatrix}$$

وهذه هي صيغة RREF للمصفوفة A. عندئذ:

$$k = 3 \text{ ، } X = \begin{bmatrix} 01 \\ 11 \\ 11 \end{bmatrix} \text{ ، } G = \left[\begin{array}{c|c} 100 & 01 \\ 010 & 11 \\ 001 & 11 \end{array}\right].$$

أعمدة G المتقدمة هي 1 ، 2 ، 3 ومن ثم تكون X هي الصفوف 1 ، 2 ، 3 على التوالي من المصفوفة H ذات الدرجة $(3-5)\times 5$. أما بقية صفوف H فهي المصفوفة المحايدة من الدرجة 2×2. وبهذا نحصل على :

$$H=\begin{bmatrix}01\\11\\11\\\hline 10\\01\end{bmatrix}$$

وتكون أعمدة H هي الأساس المنشود للشفرة $C^{\perp}$. لاحظ أيضاً أن صفوف G هي أساس للشفرة $C=\langle S\rangle$ ، وذلك استناداً إلى الخوارزمية (٢,٥,١). ▲

مثال (٢,٥,٩)

لنفرض أن $n=10$ وأن S مجموعة جزئية من K^{10} وأن صيغة RREF للمصفوفة A التي نحصل عليها من الخوارزمية (٢,٥,٧) تحتوي على الصفوف غير الصفرية التالية (صفوف G):

$$G=\begin{bmatrix}1010010101\\0001010001\\0000100100\\0000001001\\0000000011\end{bmatrix}$$

أعمدة G المتقدمة هي الأعمدة 1 ، 4 ، 5 ، 7 ، 9 ، وبعد تبديل أعمدة G لتصبح الأعمدة المتقدمة في البداية نحصل على الترتيب 10 ، 8 ، 6 ، 3 ، 2 ، 9 ، 7 ، 5 ، 4 ، 1. وبهذا نرى أن :

$$.G'=\left[\begin{array}{c|c}10000&01111\\01000&00101\\00100&00010\\00010&00001\\00001&00001\end{array}\right]$$

نكوّن الآن المصفوفة H' ونقوم بتبديل صفوفها لنحصل على المصفوفة H :

$$H = \begin{bmatrix} 01111 \\ 10000 \\ 01000 \\ 00101 \\ 00010 \\ 00100 \\ 00001 \\ 00010 \\ 00001 \\ 00001 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{matrix} \quad , \quad H' = \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} 01111 \\ 00101 \\ 00010 \\ 00001 \\ 00001 \\ 10000 \\ 01000 \\ 00100 \\ 00010 \\ 00001 \end{bmatrix} \begin{matrix} 1 \\ 4 \\ 5 \\ 7 \\ 9 \\ 2 \\ 3 \\ 6 \\ 8 \\ 10 \end{matrix}$$

وأخيراً تكون أعمدة H أساساً للشفرة $C^{\perp}$ وذلك استناداً إلى الخوارزمية (**٢,٥,٧**). ▲

تمارين

(**٢,٥,١٠**) استخدم الخوارزمية (**٢,٥,٧**) لإيجاد أساس للشفرة $C^{\perp}$ لكل من الشفرات $C = \langle S \rangle$ للمجموعات S التالية :

(أ) $S = \{010, 011, 111\}$

(ب) $S = \{1010, 0101, 1111\}$

(ج) $S = \{0101, 1010, 1100\}$

(د) $S = \{1000, 0100, 0010, 0001\}$

(هـ) $S = \{11000, 01111, 11110, 01010\}$

(و) $S = \{10101, 01010, 11111, 00011, 10110\}$

(ز) $S = \{0110, 1010, 1100, 0011, 1111\}$

(ح) $S = \{111000, 000111, 101010, 010101\}$

(ط) $S = \{00000000, 10101010, 01010101, 11111111\}$.

(**٢,٥,١١**) استخدم ترميز الخوارزمية (**٢,٥,٧**) لتفسير صواب المعادلة $GH = 0$.

(**٢,٥,١٢**) لكل من المجموعات S التالية ، عيّن أساساً B للشفرة $G = \langle S \rangle$ وأساساً $B^{\perp}$ للشفرة الثنوية $C^{\perp}$ مستخدماً الخوارزمية (**٢,٥,٧**) :

(أ) $S = \{000000, 111000, 000111, 111111\}$

(ب) $S = \{1101000, 0110100, 0011010, 0001101, 1000110, 0100011, 1010001\}$

(ج) $S = \{1111000, 0111100, 0011110, 0001111, 1000111, 1100011, 1110001\}$

(د) $S = \{101101110, 011011101, 110110010, 011011110, 111111101\}$

(هـ) $S = \{100100100, 010010010, 111111111, 000000000\}$

(و) $S = \{001101, 001000, 001111, 000101, 000001\}$

(٢,٦) المصفوفات المولّدة والتشفير

Generating Matrices & Encoding

نوظّف الآن المفاهيم التي درسناها في البنود القليلة السابقة لإيجاد مصفوفة مهمة للشفرات الخطية ونبين كيفية استخدام هذه المصفوفة لإرسال الرسائل.

نحتاج أولاً إلى بعض المفاهيم الأولية. تُعرف **رتبة مصفوفة** A **(Rank of a Matrix A)** على K ونرمز لها بالرمز $\boldsymbol{rank\ A}$ على أنها عدد الصفوف غير الصفرية في صيغة REF للمصفوفة. **بُعد الشفرة (Dimension of the Code)** C هو بُعد C كفضاء جزئي من K^n. إذا كان طول الشفرة C يساوي n وبُعدها يساوي k ومسافتها تساوي d فنقول **إنها شفرة خطية من النوع** $(\boldsymbol{n}, \boldsymbol{k}, \boldsymbol{d})$ **($(\boldsymbol{n}, \boldsymbol{k}, \boldsymbol{d})$-Linear Code)**. هذه الأعداد الثلاثة ، الطول والبُعد والمسافة هي المعلومات الأهم التي يجب معرفتها عن الشفرة C. إذا كانت C شفرة خطية طولها n وبُعدها k فنعني **بمصفوفة مولّدة (Generation Matrix)** للشفرة C ، أي مصفوفة G ، صفوفها أساس للشفرة C. لاحظ أن درجة مصفوفة مولّدة G للشفرة C هي $k \times n$ وأن رتبتها تساوي k. وبهذا نحصل على المبرهنة التالية :

مبرهنة (٢,٦,١)

تكون مصفوفة G مصفوفة مولّدة لشفرة خطية C إذا وفقط إذا كانت صفوف G مُستقلة خطياً. أي أن رتبة G تساوي عدد صفوف G. ■

وبما أن للمصفوفات المتكافئة صفياً الرتبة نفسها فإننا نحصل على المبرهنة التالية :

مبرهنة (٢,٦,٢)

إذا كانت G مصفوفة مولّدة للشفرة الخطية C فإن أي مصفوفة مكافئة صفياً للمصفوفة G هي أيضاً مصفوفة مولّدة للشفرة C. على وجه الخصوص، لأي شفرة خطية C يكون لها مصفوفة مولّدة على صيغة RREF. ■

لإيجاد مصفوفة مولّدة لشفرة خطية C نضع كلماتها كصفوف لمصفوفة A. وبما أن $C = \langle C \rangle$، نستخدم الخوارزمية (**٢,٥,١**) أو الخوارزمية (**٢,٥,٧**) لإيجاد أساس للشفرة C. عندئذ، تكون المصفوفة التي صفوفها كلمات الأساس هي مصفوفة مولّدة للشفرة C.

مثال (٢,٦,٣)

عيّن مصفوفة مولّدة للشفرة الخطية $C = \{0000, 1110, 0111, 1001\}$.

الحل

بإنشاء المصفوفة A التي صفوفها كلمات C واستخدام الخوارزمية (**٢,٥,١**) نحصل على:

$$A = \begin{bmatrix} 0000 \\ 1110 \\ 0111 \\ 1001 \end{bmatrix} \to \begin{bmatrix} 1110 \\ 0111 \\ 1001 \\ 0000 \end{bmatrix} \to \begin{bmatrix} 1110 \\ 0111 \\ 0111 \\ 0000 \end{bmatrix} \to \begin{bmatrix} 1110 \\ 0111 \\ 0000 \\ 0000 \end{bmatrix}$$

وبهذا نرى أن $G = \begin{bmatrix} 1110 \\ 0111 \end{bmatrix}$ مصفوفة مولّدة للشفرة C. أما إذا استخدمنا الخوارزمية (**٢,٥,٧**) فنجد أن صيغة RREF للمصفوفة A هي $\begin{bmatrix} 1001 \\ 0111 \\ 0000 \\ 0000 \end{bmatrix}$ وتكون $G_1 = \begin{bmatrix} 1001 \\ 0111 \end{bmatrix}$ مصفوفة مولّدة أخرى للشفرة C.

تمارين

(٢,٦,٤) بيّن أي من المصفوفتين التاليتين هي مصفوفة مولّدة لشفرة خطية.

$$A = \begin{bmatrix} 010011101 \\ 100101101 \\ 101100110 \\ 101101101 \end{bmatrix} ، \quad B = \begin{bmatrix} 1001101001 \\ 1101000101 \\ 1000010111 \\ 1010001110 \end{bmatrix}.$$

(٢,٦,٥) عيّن مصفوفة مولّدة على صيغة RREF لكل من الشفرات التالية :

(أ) $C = \{000\ ,001\ ,010\ ,011\}$

(ب) $C = \{0000\ ,1001\ ,0110\ ,1111\}$

(ج) $C = \{00000\ ,11111\}$

(د) $C = \{00000\ ,11100\ ,11100\ ,00111\ ,11011\}$

(هـ) $C = \{00000\ ,11110\ ,01111\ ,10001\}$

(و) $C = \{00000\ ,101010\ ,010101\ ,111111\}$

(٢,٦,٦) عيّن مصفوفة مولّدة لكل من الشفرات التالية ثم جد بُعد الشفرة :

(أ) $C = \{000000\ ,001011\ ,010101\ ,011110,\ 100110\ ,101101\ ,110011\ ,111000\}$

(ب) $C = \{00000000\ ,01101111\ ,11011000\ ,11111101\ ,10010010\ ,0100101\ ,01001010\ ,101101111\}$

(ج) $C = \{0000000000\ ,1111100000\ ,0000011111, 1111111111\}$

(٢,٦,٧) عيّن مصفوفة مولّدة لكل من الشفرات الخطية المولّدة بالمجموعة المبينة. جد (n,k,d) لكل من هذه الشفرات:

(أ) $S = \{11111111\ ,11110000\ ,11001100\ ,10101010\}$

(ب) $S = \{11111100\ ,11110011\ ,11001111\ ,00111111\}$

(ج) $S = \{100100100\ ,010010010\ ,001001001\ ,11111111\}$

(د) $S = \{10101\ ,01010\ ,11111\ ,00011\ ,10110\}$

(هـ) $S = \{1010\ ,0101\ ,1111\}$

(و) $S = \{101101\,, 011010\,, 110111\,, 000111\,, 110000\}$

(ز) $S = \{1001011\,, 0101010\,, 1001100\,, 0011001\,, 0000111\}$.

المبرهنة التالية تبين لنا كيفية استخدام المصفوفة المولّدة للشفرة الخطية في تشفير الرسائل.

مبرهنة (٢,٦,٨)

لنفرض أن G مصفوفة مولّدة للشفرة الخطية C ذات الطول n والبعد k. عندئذ، C هي مجموعة جميع الكلمات التي على الصورة uG حيث $u \in K^k$. أي أن $C = \{uG : u \in K^k\}$. إضافة إلى ذلك لكل $u_1, u_2 \in K^k$ نجد أن $u_1G = u_2G$ إذا وفقط إذا كان $u_1 = u_2$.

البرهان

لنفرض أن $G = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix}$ حيث $g_1, g_2, \cdots, g_k$ هي صفوف المصفوفة المولّدة G.

ولنفرض أن $v \in C$. بما أن $g_1, g_2, \cdots, g_k$ أساس للشفرة الخطية C فتوجد أعداد $a_1, a_2, \cdots, a_k \in K$ بحيث يكون:

$$v = a_1g_1 + a_2g_2 + \cdots + a_kg_k.$$

وبوضع $u = (a_1, a_2, \cdots, a_k)$ نرى أن $uG = a_1g_1 + a_2g_2 + \cdots + a_kg_k$.

إذن، $v = uG$ حيث $u \in K^k$ ومن ناحية أخرى، إذا كان $u = (a_1, a_2, \cdots, a_k) \in K^k$ فنرى أن $uG = a_1g_1 + a_2g_2 + \cdots + a_kg_k \in C$. إذن، $C = \{uG : u \in K^k\}$.

وأخيراً، إذا كان $u_1, u_2 \in K^k$ حيث $u_1 = u_2$ فمن الواضح أن $u_1G = u_2G$. وبالعكس، لنفرض أن $u_1 = (a_1, a_2, \cdots, a_k)$ وأن $u_2 = (b_1, b_2, \cdots, b_k)$ كلمتان في K^k حيث $u_1G = u_2G$. حينئذ يكون:

$$u_1G = u_2G \Rightarrow a_1g_1 + a_2g_2 + \cdots + a_kg_k = b_1g_1 + b_2g_2 + \cdots + b_kg_k$$
$$\Rightarrow (a_1 - b_1)g_1 + (a_2 - b_2)g_2 + \cdots + (a_k - b_k)g_k = 0$$

وبما أن $g_1, g_2, \cdots, g_k$ مُستقلة خطياً فنرى أن $a_i - b_i = 0$ لكل $i = 1,2,\cdots,k$. وبهذا يكون $u_1 = u_2$. ■

ملحوظة

لاحظ أن المبرهنة (**٢,٦,٨**) تنص على أن الرسائل التي يتم تشفيرها باستخدام شفرة خطية من النوع (n,k,d) هي بالضبط الرسائل $u \in K^k$ حيث يتم تشفير الرسالة u على أنها $v = uG$. وبهذا يستخدم فقط عدد k من إحداثيات أي كلمة شفرة لتشفير الرسالة. لاحظ أيضاً أن معدل المعلومات لشفرة خطية من النوع (n,k,d) هو $log_2\,(2^k)/n = k/n$.

مثال (٢,٦,٩)

لتكن C الشفرة الخطية من النوع $(5,3,d)$ حيث المصفوفة المولّدة لها هي $G = \begin{bmatrix}10110\\01011\\00101\end{bmatrix}$. عندئذ، معدل المعلومات للشفرة C هو $\frac{k}{n} = \frac{3}{5}$. وبهذا نرى أنه يمكن تشفير جميع الرسائل $u \in K^3$. فمثلاً، يتم تشفير الرسالة $u = 101$ على النحو $v = uG = [101]\begin{bmatrix}10110\\01011\\00101\end{bmatrix} = 10011$. ▲

تمارين

(**٢,٦,١٠**) لكل من المصفوفات المولّدة المعطاة شفِّر الرسائل المبينة:

(أ) $G = \begin{bmatrix}10011\\01010\\00101\end{bmatrix}$

(i) $u = 100$ (ii) $u = 010$ (iii) $u = 111$

(ب) $G = \begin{bmatrix} 1000111 \\ 0100101 \\ 0010011 \end{bmatrix}$

(i) $u = 100$ (ii) $u = 010$ (iii) $u = 111$

(ج) $G = \begin{bmatrix} 1101001 \\ 0010111 \\ 0101010 \\ 1111111 \end{bmatrix}$

(i) $u = 1000$ (ii) $u = 1010$ (iii) $u = 0011$

(iv) $u = 1011$.

(**٢,٦,١١**) لنفرض أن:

000	100	010	001	110	101	011	111
A	B	E	H	M	R	T	W

هو تقابل بين حروف الرسائل وكلمات K^3. استخدم المصفوفة المولّدة المبينة في المثال (**٢,٦,٩**) لتشفير الرسالة BE THERE (تجاهل الفراغ).

(**٢,٦,١٢**) لتكن C شفرة مصفوفتها المولّدة هي:

$$G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$$

وليكن

0000	1000	0100	0010	0001	1100	1010	1001
A	B	C	D	E	F	G	H
0110	0101	0011	1110	1101	1011	0111	1111
I	J	K	L	M	N	O	P

تقابلاً بين حروف الرسائل وكلمات K^4.

(أ) شفّر الرسالة HELP.

(ب) شفّر الرسالة HELP بافتراض وقوع الأخطاء التالية أثناء عملية الإرسال: خطأ في الإحداثي الأول من الكلمة الأولى، عدم وقوع أخطاء في الكلمة الثانية، خطأ

في الإحداثي السابع من الكلمة الثالثة، خطأ في الإحداثيين الخامس والسادس من الكلمة الرابعة.

(ج) شفّر الرسالة CALL HOME BAMA (تجاهل الفراغات).

(٢,٦,١٣) جد عدد الرسائل التي يمكن إرسالها ومعدل المعلومات r لكل من الشفرات الخطية في التمرينين **(٢,٦,٦)** و **(٢,٦,٧)**.

(٢,٧) مصفوفات اختبار النوعية

Parity-Check Matrices

نقدم الآن مصفوفة أخرى مرتبطة مع المصفوفة المولّدة للشفرات الخطية وسنوظفها في تصميم خطط فك التشفير. نقول إن مصفوفة H هي **مصفوفة اختبار (أو تحديد) النوعية (Parity-Check Matrix)** للشفرة الخطية C إذا كانت أعمدة H أساساً للشفرة الثنوية $C^{\perp}$.

إذا كانت C من الطول n والبعد k فنرى أن H من الدرجة $n \times (n-k)$ ورتبتها هي $n-k$ وذلك لأن $dimC + dimC^{\perp} = n$.

المبرهنة التالية هي رديف المبرهنة **(٢,٦,١)**.

مبرهنة (٢,٧,١)

تكون H مصفوفة اختبار النوعية لشفرة خطية C إذا وفقط إذا كانت أعمدة H مُستقلة خطياً.

البرهان[٢]

نحصل على البرهان بملاحظة أن درجة مصفوفة اختبار النوعية H لشفرة خطية من الطول n والبعد k هي $n \times (n-k)$ وأن رتبة H هي $n-k$. ■

---

(٢) المترجمان

المبرهنة التالية تصف لنا الشفرة الخطية بدلالة مصفوفة اختبار النوعية.

مبرهنة (٢,٧,٢)

إذا كانت H مصفوفة اختبار النوعية لشفرة خطية من الطول n فإن:

$$C = \{v \in K^n : vH = 0\}.$$

إذا كان لدينا مصفوفة مولّدة لشفرة خطية C فبإمكاننا إيجاد مصفوفة اختبار النوعية للشفرة C باستخدام الخوارزمية (**٢,٥,٧**) حيث إن هذه المصفوفة هي المصفوفة H المنشأة باستخدام الخوارزمية (**٢,٥,٧**)؛ لأن أعمدة H هي أساس للشفرة الثنوية $C^{\perp}$.

مثال (٢,٧,٣)

وجدنا في المثال (**٢,٦,٣**) أن $G_1 = \begin{bmatrix} 10 & 01 \\ 01 & 11 \end{bmatrix} = [I \ \ X]$ هي مصفوفة مولّدة على صيغة RREF للشفرة $C = \{0000\,,1110\,,0111\,,1001\}$ ولذا نجد استناداً إلى الخوارزمية (**٢,٥,٧**) أن:

$$H = \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

هي مصفوفة اختبار النوعية للشفرة C. لاحظ أن $vH = 00$ لكل $v \in C$. ▲

تمارين

(**٢,٧,٤**) جد مصفوفة اختبار النوعية لكل من الشفرات التالية:

(أ) $C = \{000\,,001\,,010\,,011\}$

(ب) $C = \{0000\,,1001\,,0110\,,1111\}$

(ج) $C = \{00000\,,11111\}$

(د) $C = \{00000\,,11100\,,11100\,,00111\,,11011\}$

(هـ) $C = \{00000, 11110, 01111, 10001\}$

(و) $C = \{00000, 101010, 010101, 111111\}$.

(٢,٧,٥) جد مصفوفة اختبار النوعية لكل من الشفرات التالية (المصفوفة المولّدة تم إيجادها في التمرينين (٢,٦,٦) و (٢,٦,٧)):

(أ) $C = \{000000, 001011, 010101, 011110, 100110, 101101, 110011, 111000\}$

(ب) $C = \{00000000, 01101111, 11011000, 11111101, 010010, 00100101, 01001010, 10110111\}$

(ج) $C = \{0000000000, 1111100000, 0000011111, 1111111111\}$

(د) $C = \langle S\rangle, S = \{11111111, 11110000, 11001100, 10101010\}$

(هـ) $C = \langle S\rangle, S = \{11111100, 11110011, 11001111, 00111111\}$

(و) $C = \langle S\rangle, S = \{100100100, 010010010, 001001001, 111111111\}$

(ز) $C = \langle S\rangle, S = \{10101, 01010, 11111, 00011, 10110\}$

(ح) $C = \langle S\rangle, S = \{1010, 0101, 1111\}$

(ط) $C = \langle S\rangle, S = \{101101, 011010, 110111, 000111, 110000\}$

(ي) $C = \langle S\rangle, S = 1001011, 0101010, 1001100, 0011001, 0000111\}$

نقدم الآن العلاقة بين المصفوفة المولّدة ومصفوفة اختبار النوعية للشفرات الخطية ونقدم أيضاً العلاقة بين هذه المصفوفات لشفرة خطية وثنويتها.

مبرهنة (٢,٧,٦)

تكون G مصفوفة مولّدة و H مصفوفة اختبار النوعية لشفرة خطية C إذا وفقط إذا تحقق ما يلي:

(١) صفوف G مُستقلة خطياً.

(٢) أعمدة H مُستقلة خطياً.

(٣) عدد صفوف G مضافاً إليه عدد أعمدة H يساوي عدد أعمدة G وهذا بدوره يساوي عدد صفوف H.

(٤) $GH = 0$.

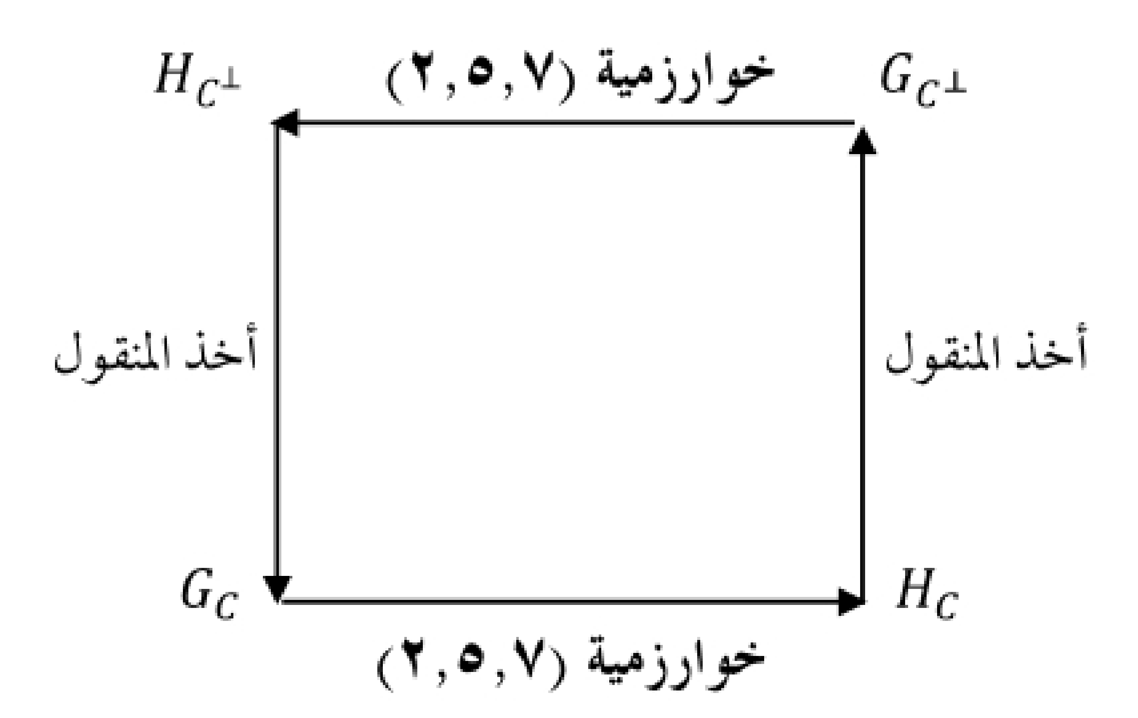
مبرهنة (٢,٧,٧)

تكون H مصفوفة اختبار النوعية لشفرة خطية C إذا وفقط إذا كانت H^T مصفوفة مولّدة للشفرة الثنوية $C^\perp$.

البرهان

نحصل على البرهان بتوظيف المبرهنة (**٢,٧,٦**) والحقيقة $H^T G^T = (GH)^T = 0$. ■

إذا كان لدينا مصفوفة مولّدة أو مصفوفة اختبار نوعية لشفرة C أو ثنويتها $C^\perp$ فيكون بإمكاننا توظيف الخوارزمية (**٢,٥,٧**) للحصول على الثلاث مصفوفات الأخرى، والمخطط التالي يوضح كيفية إنجاز ذلك



مثال (٢,٧,٨)

لتكن H مصفوفة اختبار النوعية للشفرة C حيث :

$$H = \begin{bmatrix} 11 \\ 11 \\ 01 \\ 10 \\ 01 \end{bmatrix} = \begin{bmatrix} X \\ I \end{bmatrix}$$

عندئذ ،

(أ) $H^T = \begin{bmatrix} 11010 \\ 11101 \end{bmatrix}$ مصفوفة مولّدة للشفرة الثنوية $C^{\perp}$.

(ب) $\begin{bmatrix} 11010 \\ 00111 \end{bmatrix}$ صيغة RREF للمصفوفة H^T.

ونرى استناداً إلى الخوارزمية (**٢,٥,٧**) أن مصفوفة اختبار النوعية للشفرة $C^{\perp}$ هي :

$$\begin{bmatrix} 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}.$$

(ج) باستخدام H نجد مصفوفة مولّدة للشفرة C وهي :

$$G = \begin{bmatrix} 100 & 11 \\ 010 & 11 \\ 001 & 01 \end{bmatrix} = [I \quad X]$$

وذلك باستخدام خطوات عكسية للخوارزمية (**٢,٥,٧**). وبهذا تكون :

$$G^{\top} = \begin{bmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 111 \end{bmatrix}$$

مصفوفة اختبار النوعية للشفرة الثنوية $C^{\perp}$ ، وذلك استناداً للمبرهنة (**٢,٧,٧**). ▲

تمارين

(**٢,٧,٩**) مصفوفة اختبار النوعية H لشفرة خطية C معطاة في كل فرع من فروع التمرين. جد :

(١) مصفوفة مولّدة للشفرة الثنوية $C^{\perp}$.

(٢) مصفوفة مولّدة للشفرة C.

(أ) $H = \begin{bmatrix}100\\100\\010\\001\\010\\001\end{bmatrix}$ (ب) $H = \begin{bmatrix}01\\10\\01\\10\\01\end{bmatrix}$ (ج) $H = \begin{bmatrix}111\\110\\101\\011\\100\\010\\001\end{bmatrix}$.

(**٢,٧,١٠**) جد جميع كلمات الشفرة الثنوية $C^{\perp}$ للشفرة $C = \{00000, 11111\}$ ومن ثم عيّن مصفوفة مولّدة ومصفوفة اختبار النوعية للشفرة $C^{\perp}$.

(**٢,٧,١١**) لكل من الشفرات C المبينة أدناه، جد بُعد C، بُعد $C^{\perp}$، درجة مصفوفة مولّدة ومصفوفة اختبار النوعية لكل من C و$C^{\perp}$، عدد كلمات كل من C و$C^{\perp}$، معدل المعلومات r لكل من C و$C^{\perp}$.

(أ) C من الطول $n = 2^t - 1$ وبُعد t.

(ب) C من الطول $n = 23$ والبعد 11.

(ج) C من الطول $n = 15$ والبعد 8.

(٢,٨) الشفرات المتكافئة
Equivalent Codes

لتكن $G = [I_k \quad X]$ هي المصفوفة من الدرجة $k \times n$ ، $k < n$ حيث I_k المصفوفة المحايدة من الدرجة $k \times k$. من الواضح أن G على صيغة RREF وأن صفوفها مُستقلة خطياً. إذن، G مصفوفة مولّدة لشفرة خطية طولها n وبُعدها k. نقول إن G **مصفوفة مولّدة قياسية (Standard Generating Matrix)**. كما تُسمى الشفرة الخطية C المولّدة بالمصفوفة G، **شفرة نظامية (Systematic Code)**.

ليس بالضرورة أن يكون لجميع الشفرات الخطية مصفوفة مولّدة قياسية. على سبيل المثال، الشفرة الخطية المولّدة بالمصفوفة G في التمرين (**٢,٨,١**) التالي لها إضافة إلى G خمس مصفوفات مولّدة أخرى وجميعها ليست مصفوفات مولّدة قياسية.

تمرين

(**٢,٨,١**) جد المصفوفات المولّدة الخمس الأخرى للشفرة الخطية المولّدة بالمصفوفة:

$$G = \begin{bmatrix} 100 \\ 001 \end{bmatrix}.$$

تتمتع الشفرة الخطية C التي يكون لها مصفوفة مولّدة قياسية $G = [I \quad X]$ بميزات خاصة. إحدى هذه الميزات هي استخدام الخوارزمية (**٢,٥,٧**) للحصول مباشرة على مصفوفة اختبار النوعية H للشفرة C حيث إن H في هذه الحالة هي:

$$H = \begin{bmatrix} X \\ I \end{bmatrix}.$$

ونعلم أيضاً استناداً إلى المبرهنة (**٢,٦,٨**) أنه يمكن كتابة أي كلمة v من كلمات الشفرة الخطية C ذات الطول n والبعد k على الصورة uG حيث u كلمة وحيدة من كلمات K^k و G مصفوفة مولّدة للشفرة C. يمكن التفكير في الكلمة u ذات الطول k على أنها الرسالة المرسلة ولكننا بدلاً من إرسال u فإننا بالطبع نقوم بإرسال كلمة الشفرة $v = uG$. وإذا استطاعت طريقة MLD الاستنتاج صواباً أن $v = uG$ هي الكلمة التي تم إرسالها فعندئذ، يكون من المهم على المستقبل استخدام uG للحصول على الرسالة الأصلية u. فإذا كانت G مصفوفة مولّدة قياسية فهذا يجعل الأمر بغاية السهولة وذلك لأن:

$$v = uG = u[I \quad X] = [uI \quad uX] = [u \quad uX]$$

وتكون الرسالة الأصلية u هي أول k إحداثي من كلمة الشفرة $v = uG$ ونكون قد برهنا المبرهنة التالية التي تبين إحدى الميزات المهمة لوجود مصفوفة مولّدة قياسية.

مبرهنة (٢,٨,٢)

لتكن C شفرة خطية طولها n وبُعدها k ولتكن G مصفوفة مولّدة قياسية للشفرة C. عندئذ، أول k إحداثي من كلمة الشفرة $v = uG$ هي إحداثيات الكلمة $u \in K^k$. ■

مثال (٢,٨,٣)

إذا كانت :

$$G = \begin{bmatrix} 1000 & 101 \\ 0100 & 100 \\ 0010 & 110 \\ 0001 & 011 \end{bmatrix} = [I_4 \quad X]$$

وكانت الرسالة هي $u = 0111$ فإن $uG = 0111001 = [u001]$. وأما إذا كانت $u = 1011$ فنرى أن $uG = 1011000 = [u000]$. ▲

تمارين

(**٢,٨,٤**) لتكن G هي المصفوفة المولّدة المبينة في المثال (**٢,٨,٣**). شفّر كلاً من الرسائل u التالية ثم تحقق من أن الإحداثيات الأربعة الأولى من كلمة الشفرة الناتجة هي الرسالة u.

(أ) $u = 1111$ (ب) $u = 1011$ (ج) $u = 0000$

(**٢,٨,٥**) بيّن كيفية استرداد u من uG إذا لم تكن G مصفوفة مولّدة قياسية.

(**٢,٨,٦**) إذا كانت المصفوفة المولّدة للشفرة C هي :

$$G = \begin{bmatrix} 1100101 \\ 0110101 \\ 1011011 \\ 1100110 \\ 0110000 \end{bmatrix}$$

فبيّن كيف يمكنك استرداد u من $v = uG = 0000101$.

عند توفر شروط المبرهنة (**٢,٨,٢**)، تسمى الإحداثيات k الأولى من كلمة الشفرة $v = uG$ ، **إحداثيات المعلومات (Information Digits)** ؛ لأنها بالفعل هي الرسالة u ، أما الإحداثيات $n - k$ الباقية فتسمى **الإحداثيات الزائدة أو إحداثيات اختبار النوعية (Redundancy or Parity-Check Digits)**.

مع كل هذه الميزات التي تتمتع بها شفرة خطية ذات مصفوفة مولّدة قياسية فما الذي يمكن عمله لو واجهنا شفرة خطية C ليس لها أي مصفوفة مولّدة قياسية؟ للإجابة عن هذا السؤال، دعنا نعتبر الشفرة C ذات المصفوفة المولّدة $G = \begin{bmatrix}100\\001\end{bmatrix}$ المبينة في التمرين (٢,٨,١). من السهل أن نرى أن C هي:

$$.C = \{000\,,100\,,001\,,101\}$$

وهذه شفرة خطية ليس لها مصفوفة مولّدة قياسية كما هو مبين في التمرين (٢,٨,١). لنفرض الآن أننا قمنا بإعادة ترتيب إحداثيات كل من كلمات C على النحو "الأول، الثالث، الثاني" عوضاً عن الترتيب الأصلي "الأول، الثاني، الثالث". عندئذ، نحصل على شفرة جديدة C' وهي:

$$.C' = \{000\,,100\,,010\,,110\}$$

على الرغم من أن الشفرتين C وC' مختلفتان، إلا أنهما تتشاركان في عديد من الخصائص، فمثلاً، كل منهما خطية وكل منهما من الطول 3 وبُعد كل منهما 2 ومسافة كل منهما 1. ولكن تتميز الشفرة C' عن الشفرة C بأن لها مصفوفة مولّدة قياسية G' نحصل عليها من المصفوفة G بتبديل العمودين الثاني والثالث (بالضبط كما حصلنا على C' من C). أي أن:

$$.G' = \begin{bmatrix}100\\101\end{bmatrix}$$

لتكن C شفرة قالبية من الطول n. إذا حصلنا على شفرة قالبية C' من الطول n من C بتبديل ما لإحداثيات كلمات C فعندئذ نقول إن الشفرة C' **تكافئ (Equivalent)** الشفرة C.

مثال (٢,٨,٧)

ليكن $n = 5$ ولتكن C هي الشفرة:

$$.C = \{11111\,,01111\,,00111\,,00011\,,00001\}$$

إذا استخدمنا الترتيب 3، 5، 4، 1، 2 لإحداثيات كلمات الشفرة C فنحصل على الشفرة C' المكافئة للشفرة C

$$C' = \{11111\,, 10111\,, 00111\,, 00110\,, 00010\}.$$

لاحظ أن الشفرتين غير خطيتين. ▲

مبرهنة (٢,٨,٨)

أي شفرة خطية C تكافئ شفرة خطية C' لها مصفوفة مولّدة قياسية.

البرهان

لنفرض أن G مصفوفة مولّدة للشفرة C. ضع G على صيغة RREF. أعد ترتيب أعمدة RREF بحيث تكون الأعمدة المتقدمة في البداية. عندئذ، المصفوفة الناتجة عن ذلك G' هي مصفوفة مولّدة قياسية لشفرة خطية C' تكافئ C. ■

مثال (٢,٨,٩)

المصفوفة:

$$G = \begin{bmatrix} 011000010 \\ 000100110 \\ 000010010 \\ 000001100 \\ 000000001 \end{bmatrix}$$

هي مصفوفة مولّدة على صيغة RREF وأعمدتها المتقدمة هي 9، 6، 5، 4، 2. وبإعادة ترتيب هذه الأعمدة لتأخذ الترتيب الجديد 8، 7، 3، 1، 9، 6، 5، 4، 2 نحصل على المصفوفة:

$$G' = \begin{bmatrix} 10000 & 0101 \\ 01000 & 0011 \\ 00100 & 0001 \\ 00010 & 0010 \\ 00001 & 0000 \end{bmatrix}$$

وهي مصفوفة مولّدة قياسية لشفرة خطية مكافئة للشفرة المولّدة بالمصفوفة G. ▲

تمارين

(**٢,٨,١٠**) جد شفرة نظامية C' مكافئة للشفرة C المعطاة. وتحقق من أن C وC' لهما الطول والبُعد نفسه والمسافة نفسها.

(أ) $C = \{00000, 10110, 10101, 00011\}$

(ب) $C = \{00000, 11100, 00111, 11011\}$.

(**٢,٨,١١**) جد مصفوفة مولّدة قياسية G' لشفرة مكافئة للشفرة التي لها المصفوفة المولّدة G المعطاة.

(أ) $$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(ب) $$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

(**٢,٨,١٢**) عيّن مصفوفة مولّدة قياسية G' لشفرة C' مكافئة للشفرة C التي لها مصفوفة اختبار النوعية المعطاة.

(أ) $$H = \begin{bmatrix} 110 \\ 100 \\ 010 \\ 110 \\ 101 \\ 001 \\ 011 \end{bmatrix}$$

(ب) $$H = \begin{bmatrix} 110 \\ 100 \\ 011 \\ 010 \\ 001 \end{bmatrix}.$$

(**٢,٨,١٣**) أثبت أن الشفرات المتكافئة لها الطول والبُعد نفسه والمسافة نفسها.

(**٢,٨,١٤**) بيّن فيما إذا كان كل زوج من المصفوفات G_1 و G_2 المعطاة يولّد شفرتين متكافئتين.

(أ) $$G_1 = \begin{bmatrix} 1100 \\ 0110 \\ 0011 \end{bmatrix} \quad \text{و} \quad G_2 = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}$$

(ب) $$G_1 = \begin{bmatrix} 110000 \\ 001100 \\ 000011 \end{bmatrix} \quad \text{و} \quad G_2 = \begin{bmatrix} 111111 \\ 011011 \\ 001001 \end{bmatrix}$$

(ج) $G_1 = \begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix}$ و $G_2 = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$.

(٢,٩) مسافة شفرة خطية
Distance of a Linear Code

بينَّا سابقاً أن مسافة شفرة خطية هي أصغر أوزان كلمات الشفرة غير الصفرية. سنُبين في هذا البند كيفية توظيف مصفوفة اختبار النوعية لإيجاد مسافة شفرة خطية.

مبرهنة (٢,٩,١)

لنفرض أن H مصفوفة اختبار النوعية لشفرة خطية C. عندئذ، مسافة C تساوي d إذا وفقط إذا كانت كل مجموعة عدد كلماتها $d-1$ من صفوف H مُستقلة خطياً ويوجد على الأقل مجموعة واحدة تحتوي على d من صفوف H مرتبطة خطياً.

فكرة البرهان

الفكرة وراء تبرير صواب المبرهنة (**٢,٩,١**) هي أنه إذا كانت v كلمة فإن vH تركيب خطي لصفوف من H عددها بالضبط يساوي $wt(v)$. وعليه، إذا كانت $v \in C$ حيث $wt(v) = d$ فلا بُد من وجود عدد d من صفوف H المرتبطة خطياً؛ وذلك لأن $vH = 0$. كما أن $vH = 0$ يُبين أن وزن كلمة الشفرة v يحقق المتباينة $wt(v) \geq d$. ■

مثال (٢,٩,٢)

لتكن H مصفوفة اختبار النوعية للشفرة الخطية C:

$$H = \begin{bmatrix} 110 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}.$$

بالتجريب نرى عدم وجود صفين من صفوف H مجموعهما يساوي 000 وبهذا يكون كل صفين من صفوف H مستقلين خطياً. ولكن مجموع الصفوف 4، 3، 1 يساوي 000 وبهذا فهي مرتبطة خطياً. إذن مسافة الشفرة C هي $d = 3$. ▲

تمارين

(**٢,٩,٣**) عيّن كلمات الشفرة C المقدمة في المثال (**٢,٩,٢**). احسب وزن كل من هذه الكلمات وتحقق من أن مسافة C هي $d = 3$.

(**٢,٩,٤**) احسب مسافة كل من الشفرات الخطية C التي لها مصفوفة اختبار النوعية المعطاة باستخدام المبرهنة (**٢,٩,١**) ثم تحقق من صواب إجابتك بإيجاد أوزان $wt(v)$ لكل $v \in C$.

(أ) $H = \begin{bmatrix} 0111 \\ 1110 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$ (ب) $H = \begin{bmatrix} 1110 \\ 1101 \\ 1011 \\ 0111 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$ (ج) $H = \begin{bmatrix} 0111 \\ 1110 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$.

(**٢,٩,٥**) استخدم المبرهنة (**٢,٩,١**) لإيجاد مسافة الشفرة الخطية ذات المصفوفة المولّدة التالية:

(أ) $G = \begin{bmatrix} 111000000 \\ 000111000 \\ 111111111 \end{bmatrix}$ (ب) $G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$.

(**٢,١٠**) المجموعات المشاركة

Cosets

نقدم في هذا البند مفهوماً سنوظفه في البند القادم لفك تشفير الشفرات الخطية. لتكن C شفرة خطية من الطول n ولتكن u كلمة طولها n (أي $u \in K^n$). نعرّف **المجموعة المشاركة (Coset)** للشفرة C التي تعينها الكلمة u على أنها مجموعة جميع الكلمات $v + u$ حيث $v \in C$. أي أن:

$$C + u = \{v + u : v \in C\}.$$

مثال (٢,١٠,١)

إذا كانت $C = \{000\,, 111\}$ وكانت $u_1 = 101$ ، $u_2 = 111$ ، $u_3 = 010$ فنجد أن :

$$C + u_1 = C + 101 = \{000 + 101\,, 111 + 101\} = \{101\,, 010\}$$

$$C + u_2 = C + 111 = \{000 + 111\,, 111 + 111\} = \{111\,, 000\}$$

$$C + u_3 = C + 010 = \{000 + 010\,, 111 + 010\}$$

$$= \{010\,, 101\} = C + u_1$$ ▲

تمرين

(**٢,١٠,٢**) جد المجموعات المشاركة الأخرى للشفرة $C = \{000\,, 111\}$. لاحظ أن عدد المجموعات المشاركة الممكنة للشفرة C يساوي ثمانية (مجموعة مشاركة لكل كلمة من كلمات K^3) ولكن عدد المجموعات المشاركة المختلفة يساوي أربعة فقط.

لتكن C شفرة خطية من الطول n. قد يتبادر إلى ذهن القارئ أن عدد المجموعات المشاركة المختلفة $C + u$ يساوي 2^n. أي مجموعة مشاركة لكل $u \in K^n$. ولكن كما هو مبين في المثال (**٢,١٠,١**) والتمرين (**٢,١٠,٢**) فهذا ليس صحيحاً. إذ إنه من الممكن أن تكون $u_1, u_2 \in K^n$ حيث $u_1 \neq u_2$ ولكن $C + u_1 = C + u_2$.

المبرهنة التالية تقدم عديداً من الحقائق المهمة عن المجموعات المشاركة ودراسة الأمثلة التي تلي نص المبرهنة تساعد القارئ على فهم هذه الحقائق. يحتاج برهان هذه الحقائق إلى معرفة بعض تقنيات نظرية المجموعات ولذا نتركها كتمارين للقارئ.

مبرهنة (٢,١٠,٣)

لتكن C شفرة خطية من الطول n ولتكن $u, v \in K^n$. عندئذ:

(١) إذا كانت $u \in C + v$ فإن $C + u = C + v$. أي أن كل كلمة من كلمات المجموعة المشاركة تحدد تماماً المجموعة المشاركة.

(٢) $u \in C + u$.

(٣) إذا كان $u + v \in C$ فإن $C + u = C + v$.

(٤) إذا كان $u + v \notin C$ فإن $C + u \neq C + v$.

(٥) كل كلمة من كلمات K^n محتواة في مجموعة مشاركة وحيدة للشفرة C. أي أن:

$C + u = C + v$ أو $(C + u) \cap (C + v) = \emptyset$.

(٦) $|C + u| = |C|$ لكل $u \in K^n$. أي أن عدد كلمات أي مجموعة مشاركة للشفرة C يساوي عدد كلمات الشفرة C نفسها.

(٧) إذا كان بُعد الشفرة C يساوي k فإن عدد المجموعات المشاركة المختلفة للشفرة C يساوي 2^{n-k} وعدد كلمات أي مجموعة مشاركة يساوي 2^k.

(٨) الشفرة C هي إحدى مجموعاتها المشاركة. في الحقيقة، $C = C + 0$.

مثال (٢,١٠,٤)

في هذا المثال نجد المجموعات المشاركة للشفرة:

$C = \{0000\,, 1011\,, 0101\,, 1110\}$.

بداية، C نفسها مجموعة مشاركة (**خاصية ٨**) وكل كلمة من كلمات C تحدد المجموعة المشاركة C (**الخاصتان ١ و ٥**)، ولذا نختار $u \in K^4$ حيث $u \notin C$ (ولغرض فك التشفير لاحقاً نختار u بحيث يكون وزنها أصغر ما يمكن) ولتكن $u = 1000$. عندئذ، نحصل على المجموعة المشاركة التالية بجمع u إلى كل من كلمات C:

$C + 1000 = \{1000\,, 0011\,, 1101\,, 0110\}$.

لاحظ أن $u = 1000 \in C + u = C + 1000$.

الآن، نقوم باختيار كلمة أخرى من كلمات K^4 وزنها أصغر ما يمكن ولا تنتمي إلى C أو إلى $C + 1000$ ولتكن 0100. وبهذا نجد مجموعة مشاركة جديدة:

$$.C + 0100 = \{0100\,,1111\,,0001\,,1010\}$$

وباختيار 0010 نجد المجموعة المشاركة:

$$.C + 0010 = \{0010\,,1001\,,0111\,,1100\}$$

نتوقف الآن؛ لأننا نكون قد وجدنا جميع المجموعات المشاركة المختلفة؛ وذلك لأن بُعد C هو $k = 2$. ومن ثم عدد المجموعات المشاركة المختلفة يساوي $4 = 2^2 = 2^{4-2} = 2^{n-k}$ و اتحادها يساوي K^4.

لاحظ أيضاً أن $1011 \in C$ $0001 + 1010 = 1011$. ونرى أن 0001 و 1010 تنتميان للمجموعة المشاركة نفسها، بالتحديد المجموعة المشاركة $C + 0100$ (**خاصية ٣**). ومن جهة أخرى، $0110 \notin C$ $0100 + 0010 = 0110$ وبهذا فكل من الكلمتين 0100 و 0010 تنتمي إلى مجموعة مشاركة مختلفة (**خاصية ٤**). ▲

مثال (٢,١٠,٥)

جد جميع المجموعات المشاركة للشفرة الخطية C التي لها المصفوفة المولّدة:

$$.G = \begin{bmatrix} 100110 \\ 010011 \\ 001111 \end{bmatrix}$$

الحل

بإيجاد جميع المجاميع المختلفة لصفوف G نجد أن:

$$C = \{000000\,,100110\,,010011\,,001111\,,110101\,,101001\,,011100\,,111010\}$$

المجموعات المشاركة المختلفة هي:

000000	100000	010000	001000
100110	000110	110110	101110
010011	110011	000011	011011
001111	101111	011111	000111
110101	010101	100101	111101
101001	001001	111001	100001
011100	111100	001100	010100
111010	011010	101010	110010

000100	000010	000001	000101
100010	100100	100111	100011
010111	010001	010011	010110
001011	001101	001110	001010
110001	110111	110100	110000
101101	101011	101000	101100
011000	011110	011101	011001
111110	111000	111000	111111

لاحظ أن عدد المجموعات المشاركة المختلفة يساوي 8 وأن المجموعة الأول هي C. الكلمة u التي استخدمت لإيجاد المجموعة المشاركة $C+u$ هي الكلمة العليا في كل من المجموعات المشاركة. ▲

تمارين

(**٢,١٠,٦**) جد جميع المجموعات المشاركة لكل من الشفرات الخطية التالية :

(أ) $C=\{0000\,,1001\,,0101\,,1100\}$

(ب) $C=\{0000\,,1010\,,1101\,,0111\}$

(ج) $C=\{00000\,,10100\,,01011\,,11111\}$

(د) $C=\{0000\}$.

(**٢,١٠,٧**) جد جميع المجموعات المشاركة لكل من الشفرات الخطية التالية التي لها المصفوفة المولّدة المعطاة.

(أ) $G=\begin{bmatrix}111000\\001110\\100011\end{bmatrix}$ (ب) $G=\begin{bmatrix}101010\\010101\end{bmatrix}$

(ج) $G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$ (د) $G = \begin{bmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{bmatrix}$

(هـ) $G = \begin{bmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$ (و) $G = [1111]$.

(٢,١٠,٨) جد جميع المجموعات المشاركة لكل من الشفرات الخطية التالية التي لها مصفوفة اختبار النوعية المعطاة.

(أ) $H = \begin{bmatrix} 10 \\ 11 \\ 10 \\ 01 \end{bmatrix}$ (ب) $H = \begin{bmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$ (ج) $H = \begin{bmatrix} 100 \\ 010 \\ 010 \\ 001 \\ 001 \\ 001 \end{bmatrix}$.

(٢,١٠,٩) برهن جميع فقرات المبرهنة **(٢,١٠,٣)**.

(٢,١١) MLD للشفرات الخطية

MLD for Linear Codes

أحد أهدافنا هو تصميم شفرات تتميز بسهولة وسرعة فك تشفير الكلمات المستقبلة. والشفرات الخطية تقدم لنا طريقة أكثر فاعلية لتنفيذ MLD من استخدام جدول IMLD. ولهذا الغرض، نقدم هنا طريقة لتنفيذ CMLD أو IMLD للشفرات الخطية حيث تؤدي المجموعات المشاركة ومصفوفة اختبار النوعية دوراً أساسياً في عملية فك التشفير.

لتكن C شفرة خطية ولنفرض أن كلمة الشفرة $v \in C$ قد تم إرسالها واستقبلت الكلمة w. ولنفرض أنه قد تم وقوع نمط الخطأ $u = v + w$ أثناء عملية الإرسال والاستقبال. عندئذ، يكون $w + u = v \in C$. وبهذا نرى أن نمط الخطأ u والكلمة

المستقبلة w ينتميان إلى المجموعة المشاركة نفسها للشفرة C (انظر **الخاصية ٣** من المبرهنة (**٢,١٠,٣**)).

بما أن أنماط الأخطاء المرجح وقوعها هي ذات أوزان صغيرة فإليك طريقة تنفيذ MLD لشفرة خطية C :

عند استقبالنا للكلمة w نقوم باختيار كلمة u وزنها أصغر ما يمكن في المجموعة المشاركة $C + w$ ونستنتج أن $v = w + u$ هي الكلمة المرسلة.

مثال (٢,١١,١)

لتكن $C = \{0000 , 1011 , 0101 , 1110\}$. وجدنا في المثال (**٢,١٠,٤**) مجموعات C المشاركة وهي :

0000	1000	0100	0010
1011	0011	1111	1000
0101	1101	0001	0111
1110	0110	1010	1100

لنفرض الآن أننا استقبلنا الكلمة $w = 1101$. المجموعة المشاركة $C + w = C + 1101$ التي تحتوي w هي المجموعة الثانية في القائمة السابقة. والكلمة u ذات الوزن الأصغر في المجموعة المشاركة هذه هي $u = 1000$ (هي الكلمة التي نختارها كنمط خطأ). عندئذ، نستنتج أن $v = w + u = 1101 + 1000 = 0101$ هي على الأرجح كلمة الشفرة التي أرسلت. لنفرض الآن أن $w = 1111$ هي الكلمة المستقبلة. عندئذ، توجد في المجموعة المشاركة $C + w$ التي تحتوي 1111 كلمتان وزنهما أصغر ما يمكن هما 0101 و 0001. فإذا كانت طريقة فك التشفير هي CMLD ، نقوم باختيار أي من هاتين الكلمتين ولتكن $u = 0100$ كنمط خطأ وبهذا نستنتج أن $v = w + u = 1111 + 0100 = 1011$ هي على الأرجح كلمة الشفرة التي قد تم إرسالها. ▲

تمرين

(**٢,١١,٢**) لتكن C الشفرة المبينة في المثال (**٢,١٠,٥**). استخدم طريقة CMLD لفك التشفير كل من الكلمات المستقبلة التالية:

(أ) 000011 (ب) 001001 (ج) 001101

(د) 010110 (هـ) 110101 (و) 001010

الجزء الأصعب في الطريقة الموصوفة أعلاه هو البحث عن المجموعة المشاركة التي تحتوي الكلمة المستقبلة w ومن ثم إيجاد الكلمة ذات الوزن الأصغر في المجموعة المشاركة هذه. ومن الممكن توظيف مصفوفة اختبار النوعية لإيجاد طريقة تسهل علينا هذه المهمة.

لتكن C شفرة خطية من الطول n والبعد k. ولتكن H مصفوفة اختبار النوعية للشفرة C. لكل $w \in K^n$ نعرّف **تناذر w (Syndrome of w)** على أنه الكلمة $wH \in K^{n-k}$.

مثال (٢,١١,٣)

المصفوفة H التالية هي مصفوفة اختبار النوعية للشفرة C المقدمة في المثال (**٢,١١,١**). فإذا كانت $w = 1101$ فنرى أن تناذر w هو:

$$.wH = 1101 \begin{bmatrix} 11 \\ 01 \\ 10 \\ 01 \end{bmatrix} = 11$$

لاحظ أن الكلمة ذات الوزن الأصغر في المجموعة المشاركة $C + w$ هي $u = 1000$ (انظر المثال (**٢,١١,١**)) وبهذا نرى أن تناذر u هو:

$$.uH = 1000 \begin{bmatrix} 11 \\ 01 \\ 10 \\ 01 \end{bmatrix} = 11 = wH$$

إضافة إلى ذلك، إذا كانت $w = 1101$ هي الكلمة المستقبلة فتستنتج طريقة CMLD أن:

$$v = w + u = 1101 + 1000 = 0101$$

هي كلمة الشفرة المرسلة ومن ثم نرى وقوع خطأ في الإحداثي الأول. لاحظ أيضاً أن لنمط الخطأ u يكون التناذر uH هو صف H (الصف الأول في هذه الحالة) المقابل لموقع الإحداثي الذي على الأرجح قد يكون وقع خطأ فيه. ▲

المبرهنة التالية تحتوي على بعض الحقائق الأساسية المهمة للتناذر. ويمكن برهان هذه الحقائق باستخدام تعريف المفاهيم المبينة وخصائص المجموعات المشاركة المقدمة في المبرهنة (**٢,١٠,٣**).

مبرهنة (٢,١١,٤)

لتكن C شفرة خطية من الطول n ولتكن H مصفوفة اختبار النوعية للشفرة C. إذا كانت $w, u \in K^n$ فإن:

(١) $wH = 0$ إذا وفقط إذا كانت $w \in C$.

(٢) $wH = uH$ إذا وفقط إذا كانت u وw تنتميان إلى المجموعة المشاركة نفسها للشفرة C.

(٣) إذا كان u نمط خطأ في الكلمة المستقبلة w فإن uH هو مجموع صفوف H المقابلة لمواقع وقوع الأخطاء أثناء الإرسال. ■

لاحظ أنه في حالة عدم وقوع أخطاء أثناء عملية الإرسال وإذا كانت w هي الكلمة المستقبلة فإن $wH = 0$. ولكن العكس ليس بالضرورة صحيحاً، أي من الممكن أن يكون $wH = 0$ على الرغم من وقوع أخطاء وذلك لأن كلمة الشفرة w ليس بالضرورة أن تكون هي كلمة الشفرة المرسلة.

بما أن الكلمات التي تنتمي للمجموعة المشاركة نفسها يكون لها التناذر نفسه وأن الكلمات التي تنتمي إلى مجموعات مشاركة مختلفة يكون تناذرها مختلفاً فنستطيع تحديد مجموعة مشاركة بمعرفة تناذرها حيث نعرِّف **تناذر المجموعة المشاركة (Syndrome of a Coset)** على أنه تناذر أي كلمة من كلماتها. وبهذا نرى أنه إذا كان طول الشفرة يساوي n وبُعدها يساوي k فكل كلمة طولها $n-k$ من الكلمات التي عددها 2^{n-k} يجب أن تكون تناذراً لمجموعة مشاركة واحدة فقط من المجموعات المشاركة جميعاً والتي عددها 2^{n-k}.

مثال (٢,١١,٥)

طول الشفرة C المقدمة في المثال (**٢,١١,١**) هو $n = 4$ وبُعدها هو $k = 2$. مجموعات C المشاركة (مبينة في المثال (**٢,١١,١**)) تحتوي على جميع الكلمات من الطول $n = 4$ وعددها $2^n = 2^4 = 16$. وعدد الكلمات ذات الطول $n - k = 2$ يساوي $2^{n-k} = 2^{4-2} = 2^2 = 4$. وكل من هذه الكلمات هي تناذر لمجموعة مشاركة واحدة فقط من المجموعات المشاركة للشفرة C وعددها $2^{n-k} = 4$. ▲

لحساب تناذُر مجموعة مُشاركة نقوم باختيار كلمة w في المجموعة المشاركة وعندئذ يكون تناذُرها هو wH. ولتنفيذ طريقة MLD نحتاج إلى كلمة في المجموعة المشاركة وزنها أصغر ما يمكن لاستخدامها كنمط خطأ. في الأمثلة التي تناولناها في البند السابق حرصنا على ترتيب عناصر المجموعات المشاركة لكي تكون الكلمة ذات الوزن الأصغر في الأعلى (أول كلمة من كلمات المجموعة المشاركة). تسمى أي كلمة ذات وزن أصغر في مجموعة مشاركة، **طليعة المجموعة المشاركة (Coset Leader)**. وإذا كان هناك أكثر من طليعة واحدة في مجموعة مشاركة فنختار أي واحدة منها عند تنفيذ CMLD.

مثال (٢,١١,٦)

لنفرض أن C هي الشفرة المقدمة في المثال (**٢,١١,١**). لحساب تناذر المجموعات المشاركة نقوم باختيار طليعة كل من المجموعات المشاركة ومن ثم نقوم بحساب التناذر كما هو مبين في الجدول التالي :

طليعة المجموعة المشاركة u	التناذر uH
0000	00
1000	11
0100	01
0010	10

لاحظ مرة أخرى أن كل كلمة من الطول 2 ظهرت مرة واحدة فقط كتناذر. ▲

يُسمى الجدول المبين في المثال (**٢,١١,٦**) الذي يقابل بين طلائع المجموعات المشاركة وتناذراتها ، **صفيف فك التشفير القياسي (Standard Decoding Array)** أو اختصاراً SDA. لإنشاء الجدول SDA نقوم أولاً بإيجاد المجموعات المشاركة للشفرة ومن ثم نختار طليعة u لكل منها (وهي كلمة ذات وزن أصغر في المجموعة المشاركة). بعد ذلك نجد مصفوفة اختبار النوعية H للشفرة ومن ثم نقوم بحساب uH لكل طليعة u. وطريقة أسرع لإنشاء SDA تكون باستخدام مصفوفة اختبار النوعية H لحساب المسافة d للشفرة C وتوليد جميع أنماط الأخطاء e التي تحقق $wt(e) \leq \lfloor (d-1)/2 \rfloor$ ومن ثم حساب التناذر $s = eH$ لكل منها.

مثال (٢,١١,٧)

لإنشاء جدول SDA للشفرة C المقدمة في المثال (**٢,١٠,٥**) حيث المجموعات المشاركة مبينة في المثال المذكور. لاحظ أولاً أن لكل من المجموعات المشاركة السبع الأولى كلمة طليعية واحدة فقط وهي أول كلمة في المجموعة المشاركة ، أما بالنسبة للمجموعات المشاركة الأخيرة فلها ثلاث كلمات طليعية هي 000101 ، 001010 ، 110000 ، وزن

كل منها يساوي 2. إذا أردنا استخدام طريقة CMLD فنختار أي منها ولتكن 000101 كطليعة (نمط الخطأ المفترض) للمجموعة المشاركة. أما إذا استخدمنا طريقة IMLD فنقوم بطلب إعادة إرسال ونضع علامة * في جدول SDA ليدل على ذلك. نجد الآن مصفوفة اختبار النوعية H للشفرة C:

$$H = \begin{bmatrix} 110 \\ 011 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix}.$$

وبافتراض استخدام طريقة CMLD يكون جدول SDA للشفرة C هو:

نمط الخطأ	التناذر uH
000000	000
100000	110
010000	001
001000	111
000100	100
000010	010
000001	001
000101	101

لاحظ أن التناذرات هي جميع كلمات K^3. طليعة المجموعة المشاركة C هي الكلمة الصفرية دائماً ويكون تناذُرها الكلمة الصفرية. تناذر الكلمة $u = 000101$ التي اخترناها كطليعة للمجموعة المشاركة الأخيرة هو $uH = 101$ وهذا مجموع الصفين 4 و 6 من المصفوفة H ويمثلان مواقع الإحداثي 1 في نمط الخطأ u. لو استخدمنا طريقة IMLD فنضع علامة * في هذا المكان. ▲

تمارين

(٢,١١,٨) أنشئ جدول SDA بافتراض استخدام IMLD لكل من شفرات التمرين **(٢,١٠,٦)**.

(**٢,١١,٩**) أنشئ جدول SDA بافتراض استخدام IMLD لكل من شفرات التمرين (**٢,١٠,٧**).

(**٢,١١,١٠**) أنشئ جدول SDA بافتراض استخدام IMLD لكل من شفرات التمرين (**٢,١٠,٨**).

(**٢,١١,١١**) برهن المبرهنة (**٢,١١,٤**).

بعد هذا الجهد المبذول لإنشاء جدول SDA نستطيع الآن استخدامه لفك التشفير بطريقة MLD ويتم ذلك على النحو التالي :

عند استقبالنا لكلمة w نقوم بحساب تناذُرها wH وبعد ذلك نبحث في جدول SDA لإيجاد طليعة المجموعة المشاركة u بحيث يكون $wH = uH$. وبهذا نستنتج أن كلمة الشفرة التي على الأرجح تكون قد أرسلت هي $v = w + u$.

مثال (٢,١١,١٢)

لتكن C الشفرة المبينة في المثال (**٢,١١,١**). جدول SDA أنشأناه في المثال (**٢,١١,٦**) ووجدنا مصفوفة اختبار النوعية H في المثال (**٢,١١,٣**). لنفرض أن $w = 1101$ كلمة مستقبلة. عندئذ، تناذر w هو $wH = 11$. وبالنظر إلى جدول SDA نجد أن الكلمة الطليعية u التي تحقق $wH = uH$ هي $u = 1000$ التي تقع في الصف الثاني من جدول SDA. وبهذا نستنتج أن $v = w + u = 0101$ هي كلمة الشفرة المرسلة. أما إذا كانت $w = 1111$ هي الكلمة المستقبلة فنرى أن $wH = 01 = uH$ حيث $u = 0100$ هي الكلمة الواقعة في الصف الثالث من جدول SDA. إذن، يكون فك تشفير w هو $v = w + u = 1011$. هذه النتائج تتفق مع ما وجدناه في المثال (**٢,١١,١**). ▲

لاحظ أن كلمة الشفرة $v = 0101$ هي فك تشفير الكلمة المستقبلة $w = 1101$ (في المثال السابق). وبحساب المسافات بين $w = 1101$ وكلمات الشفرة C نجد أن :

$$d(0000\,,1101) = 3 \quad , \quad d(0101\,,1101) = 1$$
$$d(1011\,,1101) = 2 \quad , \quad d(1110\,,1101) = 2$$

وبهذا نرى أن $v = 0101$ هي بالفعل أقرب كلمة شفرة إلى w.

أما في حالة الكلمة المستقبلة $w = 1111$ فكان فك تشفيرها هو $v = 1011$. وبحساب المسافات بين w وكلمات الشفرة C نجد أن :

$$d(0000\,,1111) = 4 \quad , \qquad d(0101\,,1111) = 2$$
$$d(1011\,,1111) = 1 \quad , \qquad d(1110\,,1111) = 1$$

من ذلك نرى وجود كلمتي شفرة هما الأقرب إلى $w = 1111$. وهذا ليس بالشيء المفاجئ ؛ لأن الكلمة الطليعية في المجموعة المشاركة التي تحتوي w لم تكن وحيدة. وبما أننا نستخدم طريقة CMLD ، فنختار كلمة طليعية للمجموعة المشاركة من بين كلماتها الطليعية المختلفة وهذا بدوره يؤدي إلى اختيار إحدى كلمات C الأقرب إلى w. ▲

مثال (٢,١١,١٣)

إذا كانت C هي الشفرة المقدمة في المثال (**٢,١٠,٥**) فإن جدول SDA هو المنشأ في المثال (**٢,١١,٧**). سنقوم بفك بعض التشفيرات باستخدام SDA.

لنفرض أن الكلمة المستقبلة هي $w = 110111$. عندئذ، $wH = 010$ وكلمة طليعية u تحقق $wH = uH$ هي الكلمة الواقعة في الصف السادس من جدول SDA ($u = 000010$). إذن تستنتج طريقة CMLD أن :

$$v = w + u = 110111 + 000010 = 110101$$

هي كلمة الشفرة التي تم إرسالها في هذه الحالة.

أما إذا كانت الكلمة المستقبلة هي $w = 110000$ فيكون $wH = 101 = uH$ حيث $u = 000101$ هي الكلمة الطليعية الواقعة في الصف الأخير من جدول SDA. إذن، يكون فك تشفير w هو :

$$v = w + u = 110000 + 000101 = 110101$$

لاحظ أنه لو اخترنا $u' = 001010$ ككلمة طليعية في المجموعة المشاركة الأخيرة لكان فك تشفير w هو :

$$v = w + u' = 110000 + 001010 = 111010.$$ ▲

تمارين

(**٢,١١,١٤**) إذا كانت الكلمة المستقبلة هي $w = 110000$ في المثال (**٢,١١,١٣**) وإذا اخترنا $u'' = 110000$ ككلمة طليعية للمجموعة المشاركة الأخيرة ففك تشفير w.

(**٢,١١,١٥**) لنفرض أن $w = 110111$ هي الكلمة المستقبلة في المثال (**٢,١١,١٣**). بيّن أن كلمة الشفرة $v = 110101$ هي بالفعل الأقرب إلى w.

(**٢,١١,١٦**) إذا كانت $w = 110000$ هي الكلمة المستقبلة في المثال (**٢,١١,١٣**) فجد جميع كلمات الشفرة C الأقرب إلى w.

(**٢,١١,١٧**) أعد فك التشفير للتمرين (**٢,١١,٢**) باستخدام جدول SDA المبين في المثال (**٢,١١,٧**).

(**٢,١١,١٨**) للشفرة المعطاة في المثال (**٢,١١,١٣**)، فك تشفير كل من الكلمات المرسلة w التالية:

(أ) 011101 (ب) 110101

(ج) 111111 (د) 000000.

(**٢,١١,١٩**) استخدم جدول SDA لكل من الشفرات التالية لفك تشفير الكلمات المرسلة المعطاة (جداول SDA لهذه الشفرة تم إنشاؤها في التمرينين (**٢,١١,٨**) و (**٢,١١,٩**))

(أ) $C = \{0000, 1001, 0101, 1100\}$

(i) $w = 1110$ (ii) $w = 1001$ (iii) $w = 0101$

(ب) $C = \{00000, 10100, 01011, 11111\}$

(i) $w = 10101$ (ii) $w = 01110$ (iii) $w = 10001$

(ج) $C = \{111000, 001110, 100011\}$

(i) $w = 101010$ (ii) $w = 011110$ (iii) $w = 011011$

(**٢,١١,٢٠**) لتكن H مصفوفة اختبار النوعية لشفرة C حيث:

$$H = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

فك تشفير كل من الكلمات المستقبلة w التالية:

(أ) 110100 (ب) 111111

(ج) 101010 (د) 000110

(**٢,١١,٢١**) لتكن C شفرة من الطول 7 حيث مصفوفة اختبار النوعية H هي المصفوفة من الدرجة 7×3 التي جميع كلمات صفوفها غير صفرية ومن الطول 3.

(أ) أنشئ جدول SDA للشفرة C.

(ب) فك تشفير 1010101.

يتم إنشاء جدول SDA لغرض استخدامه في فك التشفير بطريقة IMLD على النحو التالي:

لنفرض أن w هي الكلمة المستقبلة. عندئذ يكون عدد كلمات الشفرة C الأقرب إلى w مساوياً لعدد أنماط الأخطاء في المجموعة المشاركة $C + w$ ذات الوزن الأصغر. ففي حالة وجود مجموعة مشاركة للشفرة C تحتوي على أكثر من كلمة وزنها أصغري نقوم بحذف هذه المجموعة المشاركة وتناذُرها من جدول SDA. علاوة على ذلك فإن وزن كلمة طليعية في مجموعة مشاركة يساوي عدد أنماط الأخطاء التي يتم تصويبها عند استخدام طريقة MLD عند استقبالنا لكلمة تنتمي إلى المجموعة المشاركة نفسها، فإذا كان هذا الوزن كبيراً فمن الممكن اتخاذ قرار حذف المجموعة المشاركة هذه مع تناذُرها من جدول SDA (في حالة استخدام IMLD) حتى لو كانت هذه الكلمة ذات الوزن الأصغر وحيدة في المجموعة المشاركة المشار إليها. بهذا نحصل على جدول SDA

مختصر لطريقة IMLD. وفي هذه الحالة عند استقبالنا لكلمة تناذرها ليس من ضمن التناذرات التي يتكون منها جدول SDA المختصر فإننا نطلب إعادة إرسال.

عند التطبيق العملي نتعامل عادة مع شفرات عدد كلماتها كبير جداً، على سبيل المثال، ليس مفاجئاً أن يكون عدد كلمات شفرة يساوي 2^{50} ومن ثم يكون عدد صفوف جدول SDA حوالي 1.126×10^{15} مما يتسبب في صعوبة تنفيذ جدول SDA لغرض فك تشفير شفرات خطية. وبهذا يمكن القول إنه لم يتم حل مسألة فك التشفير عند الاستخدام العملي لطريقة MLD. ومع ذلك سنرى لاحقاً أن طريقة MLD فعّالة حسابياً لشفرات خطية يتم إنشاؤها بمواصفات محددة. في الحقيقة، أحد أهداف نظرية التشفير هو إنشاء شفرات يكون فك تشفيرها سهلاً بواسطة طريقة MLD.

(٢,١٢) موثوقية IMLD للشفرات الخطية

Reliability of IMLD for Linear Codes

لتكن C شفرة خطية طولها n وبُعدها k. تذكر أنه إذا تم إرسال $v \in C$ عن طريق قناة BSC باحتمال p فإن $\theta_p(C, v)$ هو احتمال استنتاج طريقة IMLD بأن الكلمة v هي بالفعل الكلمة المرسلة.

لكل كلمة طليعية وحيدة u في مجموعة مشاركة ولكل كلمة v من كلمات شفرة C تكون $v + u$ أقرب إلى v منها إلى أي كلمة شفرة أخرى. أيضاً، إذا كانت $w \neq v + u$ لكلمة v من كلمات الشفرة ولكلمة طليعية وحيدة u في مجموعة مشاركة فإنه توجد كلمة شفرة أخرى بحيث يكون قرب w منها أقل من أو يساوي قرب w من v. عندئذ، للشفرات الخطية تكون مجموعة الكلمات $L(v)$ الأقرب إلى v من كلمات الشفرة الأخرى هي:

$$L(v) = \{w : w = v + u \text{ ، هي كلمة طليعية وحيدة لمجموعة مشاركة } u\}$$

وبهذا نرى أنه إذا كانت $w = v + u$ فقيمة $\theta_p(v,w)$ تعتمد فقط على $wt(u)$. وبهذا لا تعتمد قيمة الاحتمال $\theta_p(C,v)$ على v للشفرات الخطية C. سنرمز لهذا الاحتمال المشترك بالرمز $\theta_p(C)$. عندئذ،

$$\theta_p(C) = \sum_{u \in L(0)} p^{n-wt(u)}(1-p)^{wt(u)}$$

بناء على ذلك، لإيجاد موثوقية شفرة خطية نحتاج فقط إلى معرفة الكلمات الطليعية الوحيدة للمجموعات المشاركة، حيث نقوم بحساب احتمال كل من كلمات الطليعة الوحيدة في المجموعات المشاركة باعتبارها نمط خطأ ومن ثم نأخذ مجموع هذه الاحتمالات للحصول على $\theta_p(C)$.

لاحظ أننا قد بيّنا أيضاً أن مجموعة أنماط الأخطاء التي تصوّبها الشفرات الخطية بطريقة IMLD تساوي مجموعة الكلمات الطليعية الوحيدة للمجموعات المشاركة.

مثال (٢,١٢,١)

لتكن C الشفرة المقدمة في المثال (**٢,١٠,٥**). توجد للمجموعات المشاركة كلمة طليعية واحدة وزنها 0 وست كلمات طليعية وزن كل منها يساوي 1. إذن، باستخدام IMLD نجد أن $\theta_p(C) = p^6 + 6p^5(1-p)$. ▲

تمرين

(**٢,١٢,٢**) احسب $\theta_p(C)$ لكل من شفرات التمارين (**٢,١٠,٦**)، (**٢,١٠,٧**)، (**٢,١٠,٨**).

الفصل الثالث

الشفرات التامة والشفرات ذات الصلة بها
Perfect & Related Codes

(٣,١) بعض الحدود على الشفرات
Some Bounds for Codes

نتناول الآن مسألة إيجاد عدد كلمات شفرة خطية طولها n ومسافتها d. هذه إحدى المسائل غير المحلولة للشفرات العامة ولكن يمكن حلها لبعض قيم n و d. سنجد بعض الحدود على سعة شفرة بمعرفة n و d.

إذا كان t و n عددين صحيحين حيث $0 \leq t \leq n$ فنعلم أن:

$$\binom{n}{t} = \frac{n!}{t!\,(n-t)!}$$

هو عدد المجموعات الجزئية التي عدد عناصر كل منها t التي يمكن اختيارها من مجموعة عدد عناصرها n. وبهذا نرى أن $\binom{n}{t}$ هو عدد الكلمات ذات الطول n والوزن t.

وبهذا نحصل مباشرة على الحقيقة التالية:

مبرهنة (٣,١,١)

إذا كان $0 \leq t \leq n$ وكانت v كلمة طولها n فإن عدد الكلمات ذات الطول n والتي تبعد عن v بمسافة لا تزيد عن t هو:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}. \quad \blacksquare$$

بما أن عدد جميع الكلمات ذات الطول n يساوي 2^n فبوضع $t = n$ في المبرهنة (٣,١,١) نرى أن :

$$.\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$$

تمرين

(٣,١,٢) لتكن $v = 10110$ و $t = 3$. تحقق من صواب المبرهنة (٣,١,١) بإيجاد جميع كلمات K^5 التي بُعدها عن v هو على الأكثر 3 ومن ثم تحقق من أننا نستطيع الحصول على هذا العدد من الكلمات بتطبيق المبرهنة (٣,١,١).

لإيجاد جميع الكلمات التي تبعد مسافة t عن كلمة معينة v نقوم بإيجاد المجاميع $v + w$ لكل الكلمات w ذات الوزن t. فإذا كان طول الشفرة C يساوي n ومسافتها هي $d = 2t + 1$ فلا توجد أي كلمة w تبعد مسافة على الأكثر t من كلمتي شفرة v_1 و v_2 مختلفتين. ولرؤية ذلك لاحظ أنه إذا كان $d(w, v_1) \leq t$ و $d(w, v_2) \leq t$ حيث $v_1 \neq v_2$ فنرى أن :

$$d(v_1, v_2) \leq d(v_1, w) + d(w, v_2) \leq 2t < d = 2t + 1$$

وهذا يناقض تعريف مسافة الشفرة C. مما سبق نرى أنه إذا كان طول الشفرة C يساوي n ومسافتها تساوي $d = 2t + 1$ فإن مجموعة جميع كلمات K^n التي تبعد مسافة t على الأكثر من كلمة شفرة v_1 لا تتقاطع مع مجموعة كلمات الشفرة التي تبعد بمسافة على الأكثر t من كلمة شفرة أخرى v_2 حيث $v_1 \neq v_2$ وبهذا نكون قد أثبتنا المبرهنة التالية :

مبرهنة (٣,١,٣) [حد هامينغ Hamming Bound]

إذا كانت C شفرة طولها n ومسافتها $d = 2t + 1$ أو $d = 2t + 2$ فإن :

$$.|C|\left[\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}\right] \leq 2^n$$

أي أن :

$$.|C| \leq \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}$$ ■

إن حد هامينغ هو حد أعلى لعدد كلمات شفرة (سواء أكانت خطية أم لا) طولها n ومسافتها $d = 2t + 1$. وبما أن $t = \lfloor (d-1)/2 \rfloor$ فنجد استناداً إلى المبرهنة (١,١٢,٩) أن مثل هذه الشفرات تُصوّب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن t.

مثال (٣,١,٤)

إذا كانت C شفرة خطية طولها $n = 6$ ومسافتها $d = 3$ $(d = 3 = 2(1) + 1)$ فنرى أن:

$$.|C| \leq \frac{2^6}{\binom{6}{0}+\binom{6}{1}} = \frac{64}{1+6} = \frac{64}{7}$$

وبما أن $|C|$ قوة للعدد 2 فيكون $|C| \leq 8$ وبهذا نجد أن $k = dimC \leq 3$. ▲

تمارين

(**٣,١,٥**) جد حداً أعلى لبعد الشفرة الخطية لقيم n و d المعطاة.

(أ) $n = 8$ ، $d = 3$ (ب) $n = 7$ ، $d = 3$

(ج) $n = 10$ ، $d = 5$ (د) $n = 15$ ، $d = 3$

(هـ) $n = 15$ ، $d = 5$ (و) $n = 23$ ، $d = 7$.

(**٣,١,٦**) تحقق من صحة حد هامينغ للشفرات الخطية التي لها المصفوفة المولّدة التالية:

(أ) $G = \begin{bmatrix} 111110000000000 \\ 000001111100000 \\ 000001111111111 \end{bmatrix}$ (ب) $G = \begin{bmatrix} 100111 \\ 010101 \\ 001011 \end{bmatrix}$

(ج) $G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$.

نعلم من البند (٢,٧) والمبرهنة (٢,٩,١) أن مصفوفة اختبار النوعية H لشفرة خطية من النوع (n,k,d) هي مصفوفة من الدرجة $n \times (n-k)$ بحيث يكون أي $d-1$

صفاً من صفوفها مُستقلة خطياً. وبما أن طول كل من صفوفها يساوي $n - k$ فيستحيل وجود أكثر من $n - k$ من الصفوف المُستقلة خطياً. إذن، $d - 1 \le n - k$. أي $k < n - d + 1$

ونكون قد برهنا النتيجة التالية التي تسمى **حد سينغلتون (Singleton Bound)**:

مبرهنة (٣,١,٧) [حد سينغلتون Singleton Bound]

إذا كانت C شفرة خطية من النوع (n, k, d) فإن $d - 1 \le n - k$. ■

لاحظ أن حد سينغلتون أضعف من حد هامينغ، فمثلاً، إذا كان $n = 15$ و $d = 5$ فإن $k \le 11$ استناداً إلى المبرهنة (٣,١,٧) وإن $k \le 8$ استناداً إلى حد هامينغ. وعلى الرغم من ذلك، يوجد صنف مهم من الشفرات تُدعى الشفرات ذات المسافة العظمى القابلة للفصل وهذه شفرات تتحقق فيها المساواة لحد سينغلتون. نقول إن الشفرة الخطية من النوع (n, k, d) شفرة قابلة للفصل بالمسافة العظمى **(Maximum Distance Separable)** أو اختصاراً شفرة MDS إذا كان $d = n - k + 1$ أو $(k = n - d + 1)$.

المبرهنة التالية تزودنا ببعض التمييزات المتكافئة لشفرات MDS.

مبرهنة (٣,١,٨)

العبارات التالية متكافئة للشفرات الخطية C من النوع (n, k, d):

(١) $d = n - k + 1$.

(٢) أي $n - k$ من صفوف مصفوفة اختبار النوعية مُستقلة خطياً.

(٣) أي k من أعمدة مصفوفة مولّدة مُستقلة خطياً.

(٤) C هي شفرة MDS.

البرهان

باستخدام المبرهنة (٣,١,٧) نعلم أن $d \le n - k + 1$. ولكن $d \le n - k + 1$ إذا وفقط إذا كان $n - k$ صفاً من صفوف مصفوفة اختبار النوعية مُستقلة خطياً. إذن، (١) تُكافئ (٢). ولإثبات أن (١) تُكافئ (٣) لاحظ أنه إذا كان $d = n - k + 1$ فلا توجد

كلمة شفرة غير صفرية تحتوي على أكثر من $k-1$ إحداثي صفري. ولكن من السهل إثبات أن أي k من أعمدة مصفوفة مولّدة من الدرجة $k\times n$ مرتبطة خطياً إذا وفقط إذا وجدت كلمة شفرة غير الصفرية تحتوي عدد k من الإحداثيات الصفرية في هذه المواقع (أثبت هذه العبارة). ■

نتيجة (٣,١,٩)

الشفرة الثنوية لشفرة MDS من النوع $(n,k,n-k+1)$ هي شفرة MDS من النوع $(n,n-k,k+1)$. ■

سنعطي أمثلة على شفرات MDS عند دراستنا لشفرات ريد وسولومن.

تمارين

(**٣,١,١٠**) الأعمدة 5 ، 3 ، 2 من المصفوفة المولّدة مرتبطة خطياً.

$$G=\begin{bmatrix}11001\\01110\\00101\end{bmatrix}$$

عيّن كلمة شفرة تكون الإحداثيات 5 ، 3 ، 2 فيها صفرية.

(**٣,١,١١**) إذا كانت k من أعمدة مصفوفة مولّدة من الدرجة $k\times n$ مرتبطة خطياً فأثبت وجود كلمة شفرة غير صفرية إحداثياتها أصفار في هذه المواقع.

هدفنا الآن محاولة إنشاء شفرات لأعداد معطاة d ، k ، n. فمثلاً، إذا كان $n=15$ و $d=5$ فاستناداً إلى حد هامينغ لا توجد شفرة يكون بُعدها $k=10$ ولكن هذا الحد لا يمنع وجود شفرة من النوع (15,8,5). فهل نستطيع إيجاد شفرة من النوع (15,8,5)؟ إن حل هذه المسألة بصورة عامة عادة ما يكون صعباً جداً ولكن إحدى الطرق التي يمكن اتباعها هي إيجاد مصفوفة اختبار النوعية لمثل هذه الشفرات. أي بفرض أن $r=n-k$، نحاول إيجاد عدد n من المتجهات طول كل منها r لتكون صفوفاً للمصفوفة H على شرط أن تكون أي مجموعة من المتجهات عددها $d-1$ مُستقلة خطياً.

مثال (٣,١,١٢)

لنفرض أن $n = 15$، $k = 6$، $d = 5$. عندئذ، $r = 15 - 6 = 9$. وبهذا نرغب في إيجاد 15 متجهاً غير صفري طول كل منها 9 بحيث يكون أي 4 متجهات منها مُستقلة خطياً. إيجاد المتجهات التسعة الأولى منها عملية سهلة حيث من الممكن اعتبارها صفوف المصفوفة المحايدة I_9 من الدرجة 9×9. لنفرض الآن أننا استطعنا إيجاد ثلاثة متجهات أخرى بطريقة ما ليصبح عدد المتجهات التي وجدناها يساوي 12. وبهذا تكون:

$$H = \begin{bmatrix} I_9 \\ 111100000 \\ 100011100 \\ 101000011 \\ ? \end{bmatrix}$$

قبل الشروع في محاولة إيجاد متجه آخر لاحظ أنه من الممكن إثبات وجود مثل هذا المتجه على النحو التالي: لا يمكن أن يكون هذا المتجه صفرياً أو من المتجهات الاثني عشر التي تم اختيارها سابقاً من بين جميع المتجهات والتي عددها 2^9. كما أن هذا المتجه لا يمكن أن يكون مجموع متجهين أو ثلاثة متجهات من المتجهات التي تم اختيارها؛ لأن ذلك يؤدي إلى مجموعة مرتبطة خطيّاً مكوّنة من 3 أو 4 متجهات. وهذا يستثني اختيار $\binom{12}{3} + \binom{12}{2}$ متجهاً على الأكثر.

وباستثناء الشروط السابقة يكون بإمكاننا اختيار أي متجه مما تبقى من المتجهات. وبما أن:

$$1 + \binom{12}{1} + \binom{12}{2} + \binom{12}{3} < 2^9$$

فنرى أن مثل هذا المتجه موجود. على سبيل المثال، من الممكن اختيار المتجه 010101010 ليكون الصف الثالث عشر للمصفوفة H. نترك عملية اختيار الصفين الأخيرين من المصفوفة H للتمرين (٣,١,٢١).

يُبيّن لنا المثال (**٣,١,١٢**) (والتمارين ذات العلاقة) وجود شفرات من النوع (15,6,5). وهذا بدوره يُزودنا بحد أدنى للسعة العظمى (أو لأكبر بُعد) لشفرة خطية تُحقق $n = 15$ ، $d = 5$. أي أن $6 \leq k \leq 8$.

المبرهنة التالية تعميم للمثال (**٣,١,١٢**) لإنشاء شفرات خطية (ومن ثم إيجاد حدود دُنيا) ونترك إثباتها للتمرين (**٣,١,٢٢**).

مبرهنة (٣,١,١٣) [حد جلبرت وڤارشاموڤ Gilbert-Varshamov Bound]

إذا كان $\binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{d-1} < 2^{n-k}$ فتوجد شفرة خطية من النوع (n, k, d). ■

نتيجة (٣,١,١٤)

إذا كان$n \neq 1$ و $d \neq 1$ فتوجد شفرة خطية C طولها n ومسافتها على الأقل d وتحقق:

$$|C| \geq \frac{2^{n-1}}{\binom{n-1}{0}+\binom{n-1}{1}+\cdots+\binom{n-1}{d-2}}. \quad ■$$

مثال (٣,١,١٥)

هل توجد شفرة خطية طولها $n = 9$ وبُعدها $k = 2$ ومسافتها $d = 5$ ؟

الحل

لاحظ أن:

$$\binom{n-1}{0} + \cdots + \binom{n-1}{d-2} = \binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \binom{8}{3} = 93$$

وأن $2^{n-k} = 2^{9-2} = 2^7 = 128$. وبما أن $93 < 128$ فنرى استناداً إلى حد جلبرت وڤارشاموڤ وجود مثل هذه الشفرة الخطية. ▲

مثال (٣,١,١٦)

جد حداً أدنى وحداً أعلى لبعد الشفرة الخطية k حيث $n = 9$ و $d = 5$.

الحل

باستخدام النتيجة (**٣,١,١٤**) نجد أن حد أدنى لعدد عناصر الشفرة C هو :

$$|C| \geq \frac{2^{n-1}}{\binom{n-1}{0}+\cdots+\binom{n-1}{d-2}} = \frac{2^{9-1}}{\binom{8}{0}+\binom{8}{1}+\binom{8}{2}+\binom{8}{3}} = \frac{2^8}{93} = \frac{256}{93} = 2.75.$$

ولكن C خطية ومن ثم فإن $|C|$ قوة للعدد 2. وبهذا يكون $|C| \geq 4$.

ولإيجاد حد أعلى للعدد $|C|$ نستخدم حد هامينغ فنجد :

$$|C| \leq \frac{2^9}{\binom{9}{0}+\binom{9}{1}+\binom{9}{2}} = \frac{512}{1+9+36} = \frac{512}{46} = 11.13.$$

ولكن C شفرة خطية ومن ثم $|C|$ قوة للعدد 2. وبهذا يكون $|C| \leq 8$. مما سبق نجد أن $2^2 \leq |C| \leq 2^3$. أي أن $2 \leq k \leq 3$. وبهذا توجد شفرات خطية من النوع (9,2,5) و (9,3,5) ولكن لا توجد شفرات خطية من النوع $(9, k, 5)$ حيث $k > 3$. ▲

مثال (٣,١,١٧)

هل توجد شفرة خطية من النوع (15,7,5)؟

الحل

باستخدام حد جلبرت وڤارشاموف نرى أن :

$$\binom{n-1}{0} + \cdots + \binom{n-1}{d-2} = \binom{14}{0} + \binom{14}{1} + \binom{14}{2} + \binom{14}{3}$$
$$= 1 + 14 + 91 + 364 = 470$$

وأن $2^{n-k} = 2^{15-7} = 256$. وبما أن $256 < 470$ فنجد أن حد جلبرت وڤارشاموف غير مُحقق ومن ثم فلا نستطيع الجزم بوجود أو عدم وجود مثل هذه الشفرات. سنرى لاحقاً أن مثل هذه الشفرة موجودة وهي مثال على شفرة BCH التي تُصوّب خطأين. ▲

تمارين

(**٣,١,١٨**) لكل فقرة من فقرات التمرين (**٣,١,٣**) ضع $k = 2d$ ثم قرر وجود أو عدم وجود شفرة تحقق المطلوب. وفي حالة عدم تقييد k، جد حداً أدنى وحداً أعلى لعدد كلمات الشفرة.

(**٣,١,١٩**) جد حداً أدنى وحداً أعلى لعدد كلمات الشفرات الخطية ذات الطول n والمسافة d لما يلي :

(أ) $n = 15$ ، $d = 5$ (ب) $n = 15$ ، $d = 3$

(ج) $n = 11$ ، $d = 3$ (د) $n = 12$ ، $d = 3$

(هـ) $n = 12$ ، $d = 4$ (و) $n = 12$ ، $d = 5$.

(**٣,١,٢٠**) هل من الممكن إيجاد شفرة خطية من النوع (8,3,5) ؟

(**٣,١,٢١**) جد شفرة من النوع (15,6,5) بإنشاء مصفوفة اختبار النوعية (انظر المثال (**٣,١,١٢**) ولاحظ أن وزن كل من الكلمات الثلاث الباقية يجب أن يكون على الأقل 4. لماذا ؟)

(**٣,١,٢٢**) لتكن H_i مصفوفة من الدرجة $i \times (n-k)$ حيث أي $d-1$ من صفوفها مُستقلة خطياً.

(أ) أثبت أنه يوجد على الأكثر $N_i = \binom{i}{0} + \binom{i}{1} + \cdots + \binom{i}{d-1}$ كلمة في المجموعة K^{n-k} بحيث تكون كل منها تركيباً خطياً لعلى الأكثر $d-2$ صفاً من صفوف H_i.

(ب) إذا كان $N_i < 2^{n-k}$ فبرهن أنه يمكن إضافة صف بحيث يكون أي $d-1$ من صفوف المصفوفة الناتجة عن ذلك مُستقلة خطياً.

(ج) أثبت حد جلبرت وڤارشاموف.

(د) أثبت النتيجة (**٣,١,١٤**).

(٣,٢) الشفرات التامة

Perfect Codes

نقول إن الشفرة C من الطول n والمسافة الفردية $d = 2t + 1$ هي **شفرة تامة (Perfect Code)** إذا حققت المساواة في حد هامينغ المبين في المبرهنة (**٣,١,٣**). أي إذا كان :

$$|C| = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}.$$

على الرغم من عدم وجود عدد كبير من الشفرات الخطية التامة إلا ان لهذا العدد القليل من الشفرات الخطيّة التامة أهمية كبيرة. الجزء الأهم في إنشاء شفرة خطية تامة يكمن في التحقق من أن العدد $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}$ هو قوة للعدد 2 ؛ (لأن $|C|$ قوة للعدد 2).

مثال (٣,٢,١)

أثبت أن $C = K^n$ شفرة تامة.

الحل

لاحظ أن مسافة K^n هي $d = 1 = 2(0) + 1$ ومن ثم فإن $t = 0$. ونرى أن:

$$\frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}} = \frac{2^n}{\binom{n}{0}} = 2^n = |K^n|$$

وبهذا تكون K^n شفرة تامة. ▲

مثال (٣,٢,٢)

إذا كانت C شفرة تامة حيث طولها ومسافتها متساويان ويساوي كل منهما $2t+1$ فأثبت أن C تحتوي على كلمتين فقط.

الحل

لنفرض أن $n = d = 2t + 1$. عندئذ،

$$\binom{n}{n-i} = \frac{ni}{(n-i)!(n-(n-i))!} = \frac{n!}{(n-i)!i!} = \binom{n}{i}.$$

وبهذا نرى أن:

$$\binom{n}{0} = \binom{n}{n}, \binom{n}{1} = \binom{n}{n-1}, \binom{n}{2} = \binom{n}{n-2}, \cdots,$$

وبوضع $n = 2t + 1$ نجد:

$$\binom{n}{t} = \binom{n}{n-t} = \binom{n}{t+1}$$

وبهذا يكون :

$$\binom{n}{0}+\cdots+\binom{n}{t}=\frac{1}{2}\left(\binom{n}{0}+\cdots+\binom{n}{n}\right)=\frac{1}{2}\cdot 2^n=2^{n-1}$$

إذن ، $|C|=\frac{2^n}{\binom{n}{0}+\cdots+\binom{n}{t}}=\frac{2^n}{2^{n-1}}=2$.

لاحظ أن شفرة التكرار $C=\{00,11\}$ هي الشفرة الخطية التامة الوحيدة التي تحتوي على كلمتين فقط. ▲

الشفرتان المقدمتان في المثالين (**٣,٢,١**) و (**٣,٢,٢**) هما شفرتان تامتان، ولكن لا توجد لهما فائدة تُذكر عند التطبيق العملي ولهذا السبب يُطلق عليهما **الشفرتان التامتان التافهتان (Trivial Perfect Codes)**.

مثال (٣,٢,٣)

إذا كان $n=7$ و $d=3$ فنرى أن $t=1$ وأن :

$$|C|=\frac{2^7}{\binom{7}{0}+\cdots+\binom{7}{1}}=\frac{128}{8}=16=2^4.$$

وبهذا نرى إمكانية وجود شفرة خطية تامة طولها $n=7$ ومسافتها $d=3$. هذه الشفرة موجودة وتُسمى **شفرة هامينغ (Hamming Code)** وسنقدمها في البند القادم. ▲

مثال (٣,٢,٤)

إذا كان $n=23$ و $d=7$ فإن $t=3$ وإن :

$$|C|=\frac{2^{23}}{\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}}=\frac{2^{23}}{1+23+253+1771}$$

$$=\frac{2^{23}}{2048}=\frac{2^{23}}{2^{11}}=2^{12}=4096$$

وهذا يُبين إمكانية وجود شفرة خطية تامة طولها $n=23$ ومسافتها $d=7$. سنرى في بند قادم أن مثل هذه الشفرة موجودة وتُسمى **شفرة غوليه (Golay Code)**. ▲

تمارين

(٣,٢,٥) إذا كان $n = 2^r - 1$ فأثبت أن $\binom{n}{0} + \binom{n}{1} = 2^r$.

(٣,٢,٦) هل توجد شفرة تامة للقيم n و d التالية:

(أ) $n = 15$، $d = 3$ (ب) $n = 31$، $d = 3$

(ج) $= 15$ ، $d = 5$ ؟

لقد تم إيجاد القيم والمسافات الممكنة للشفرات التامة من قبل **تيتاڤايرن وڤان لنت** (**Tietärväiren and Van Lint**) في العام ١٩٧٣م ولكن برهان ذلك يُخرجنا عن نطاق هذا الكتاب.

مبرهنة (٣,٢,٧)

إذا كانت C شفرة تامة غير تافهة طولها n ومسافتها $d = 2t + 1$ فإما أن $n = 23$ و $d = 7$ أو أن $n = 2^r - 1$ حيث $r \geq 3$ و $d = 3$. ■

مبرهنة (٣,٢,٨)

إذا كانت C شفرة خطيّة تامة طولها n ومسافتها $d = 2t + 1$ فإن C تُصوّب فقط جميع أنماط الأخطاء التي أوزانها لا تزيد عن t.

البرهان

لنفرض أن C شفرة خطية طولها n ومسافتها $d = 2t + 1$. بيّنا في المبرهنة (**١,١٢,٩**) أن C تُصوّب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $t = (d - 1)/2$. ولهذا فكل كلمة طولها n ووزنها لا يزيد عن t هي كلمة طليعية لمجموعة مشاركة. وعدد هذه الكلمات يساوي:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}.$$

ولكن هذا العدد ما هو إلاّ عدد المجموعات المشاركة للشفرات التامة. ■

لاحظ أنه من الممكن إعادة صياغة نص المبرهنة (**٣,٢,٨**) ليكون:

كل من كلمات K^n والتي عددها 2^n تبعد مسافة t عن كلمة شفرة واحدة فقط.

هذه الخاصية تساعدنا على حساب عدد كلمات الشفرة ذات الوزن الأصغر غير الصفري للشفرة التامة. الشفرة التامة التي تُصوّب جميع أنماط الأخطاء ذات الأوزان الذي لا تزيد عن t تُدعى **شفرة تامة من الدرجة t في تصويب الأخطاء** (**Perfect *t*- Error Correcting Code**). ومن المبرهنة (**٣,٢,٧**) نجد أن قيم t الممكنة هي $t = 1$ و $t = 3$. سندرس الحالة $t = 1$ في البند التالي.

(٣,٣) شفرات هامينغ

Hamming Code

نحن الآن جاهزون لتصميم شفرة. ندرس عائلة مهمة من الشفرات التي من السهل تشفير كلماتها وفك تشفيرها والتي تُصوّب جميع أنماط الأخطاء ذات الخطأ الواحد.

لتكن C شفرة من الطول $n = 2^r - 1$ حيث $r \geq 2$ ولتكن H مصفوفة اختبار النوعية للشفرة C. إذا كانت جميع صفوف H متجهات غير صفرية من الطول r فنقول إن C **شفرة هامينغ** (**Hamming Code**) من الطول $2^r - 1$.

مثال (**٣,٣,١**)

المصفوفة H التالية هي أحد خيارات مصفوفات اختبار النوعية لشفرة هامينغ من الطول $7(r = 3)$:

$$H = \begin{bmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

وباستخدام الخوارزمية (٢,٥,٧) تستطيع إيجاد مصفوفة مولّدة G لشفرة هامينغ من الطول 7 وهي:

$$G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}.$$

وبهذا نرى أن بُعد الشفرة يساوي 4 وعدد كلمات الشفرة يساوي $16 = 2^4$. وبتوظيف المبرهنة (٢,٩,١) نجد أن مسافة الشفرة هي $d = 3$. معدل المعلومات يساوي $4/7$. ولقد قمنا في التمرين (٢,٦,١٢) بتشفير بعض الرسائل باستخدام هذه الشفرة. كما توجد خيارات أخرى لمصفوفة اختبار النوعية لشفرة هامينغ من الطول 7 وجميعها تولّد شفرات متكافئة. ▲

بملاحظة أن مصفوفة اختبار النوعية H لشفرة هامينغ C تحتوي جميع الصفوف من الطول r التي وزن كل منها يساوي 1 (لاحظ أن عدد هذه الصفوف يساوي r)، نرى أن أعمدة H وعددها r مُستقلة خطياً. إذن، بُعد شفرة هامينغ يساوي $2^r - 1 - r$ وعدد كلماتها يساوي 2^{2^r-1-r}.

بما أن جميع صفوف H هي كلمات غير صفرية فلا يوجد صف واحد من صفوف H مرتبط خطياً. وتكون مسافة C على الأقل 2. وبما أنه لا يوجد صفان متساويان من صفوف H فنرى أن أي صفين يجب أن يكونا مستقلين خطياً. ولهذا تكون مسافة C هي على الأقل 3. ولكن H تحتوي على الصفوف:

$$\begin{matrix} 100\cdots0 \\ 010\cdots0 \\ 110\cdots0 \end{matrix}$$

وهي مجموعة مرتبطة خطياً. إذن، استناداً إلى المبرهنة (٢,٩,١) نرى أن مسافة شفرة هامينغ هي $d = 3$. لدينا الآن، $n = 2^r - 1$ و $d = 2t + 1 = 3$ (أي أن $t = 1$). وبهذا نرى أن:

$$|C| = 2^{2^r-1-r} = \frac{2^{2^r-1}}{1+2^r-1} = \frac{2^{2^r-1}}{1+n} = \frac{2^n}{\binom{n}{0}+\binom{n}{1}} = \frac{2^n}{\binom{n}{0}+\cdots+\binom{n}{t}}.$$

وبهذا تكون شفرة هامينغ شفرة تامة. إذن، استناداً إلى المبرهنة (**٣,٢,٨**) تكون شفرة هامينغ شفرة تامة تُصوّب خطأ واحداً فقط.

من السهل أيضاً إنشاء جدول SDA لشفرة هامينغ. بما أن أي خطأ واحد يتم تصويبه فنرى أن جميع الكلمات ذات الطول $2^r - 1$ وذات الوزن 1 هي أنماط أخطاء يتم تصويبها ومن ثم فهي كلمات طليعية للمجموعات المشاركة. وإذا كان e نمط خطأ فيكون eH حاصل جمع صفوف مصفوفة اختبار النوعية H التي تقابل المواقع التي وقعت فيها الأخطاء. وبما أن عدد صفوف H يساوي $2^r - 1$ فإن جدول SDA لشفرة هامينغ يأخذ الشكل:

الكلمة الطليعية	التناذر
$000\cdots0$	$000\cdots0$
I_{2^r-1}	H

مثال (٣,٣,٢)

استخدم شفرة هامينغ المقدمة في المثال (**٣,٣,١**) لفك تشفير $w = 1101001$.

الحل

التناذُر هو $wH = 011$ وهو الصف الرابع من صفوف H. وبهذا تكون الكلمة الطليعية u هي الصف الرابع من I_7 وهي $u = 0001000$. إذن، فك تشفير w هو:

$$w + u = 1100001.$$ ▲

تمارين

(**٣,٣,٣**) جد مصفوفة مولّدة قياسية لشفرة هامينغ من الطول 15 واستخدمها لتشفير الرسالة 11111100000000.

(**٣,٣,٤**) أنشئ جدول SDA لشفرة هامينغ من الطول 7 واستخدمه لفك تشفير الكلمات التالية:

(أ) 1101011 (ب) 1111111

(ج) 0011010 (د) 0101011

(هـ) 0100011 (و) 0001011

(**٣,٣,٥**) أنشئ جدول SDA لشفرة هامينغ من الطول 15 واستخدمه لتشفير الكلمات التالية

(أ) 01000 01010 01010 (ب) 10110 00101 11110

(ج) 00111 01110 11100 (د) 00000 10110 11100

(هـ) 00110 10100 00011 (و) 11000 11001 11001.

(**٣,٣,٦**) أثبت أن كلاً من المصفوفتين التاليتين هي مصفوفة اختبار النوعية لشفرة هامينغ من الطول 7 وأن كلاً من الشفرتين تكافئ الشفرة المقدمة في المثال (**٣,٣,١**):

$$H'' = \begin{bmatrix} 100 \\ 110 \\ 111 \\ 011 \\ 101 \\ 010 \\ 001 \end{bmatrix} \quad , \quad H' = \begin{bmatrix} 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{bmatrix}.$$

(**٣,٣,٧**) أثبت أن جميع شفرات هامينغ ذات الطول نفسه متكافئة.

(**٣,٣,٨**) هل المصفوفة التالية هي منقول مصفوفة اختبار النوعية لشفرة هامينغ من الطول 15؟

$$H^T = \begin{bmatrix} 10001 & 10111 & 01000 \\ 11100 & 10001 & 11110 \\ 01011 & 00101 & 11101 \\ 10001 & 01011 & 00111 \end{bmatrix}$$

(**٣,٣,٩**) أثبت أن شفرة هامينغ ذات الطول $2^r - 1$ حيث $r = 2$ هي شفرة تافهة.

(**٣,٣,١٠**) استخدم شفرة هامينغ من الطول 7 المقدمة في المثال (**٣,٣,١**) والتقابل بين الرسائل وحروف الهجاء المبين في المثال (**٢,٦,١٢**) لفك تشفير الرسالة التالية :

1010111 , 0110111 , 1000010 , 0010101 , 1001011 , 0010000 , 1111100.

(٣,٤) الشفرات الممتدة
Extended Codes

زيادة طول شفرة بإضافة إحداثي واحد أو بعض الإحداثيات تؤدي أحياناً إلى الحصول على شفرات جديدة تكون قدرتها على اكتشاف وتصويب الأخطاء أفضل من الشفرة الأصلية مما يستحق التضحية الناتجة عن الانخفاض في معدل المعلومات. نُقدم في هذا البند أحد التمديدات البسيطة.

لنفرض أن C شفرة من الطول n ولنفرض أن C^* شفرة من الطول $n+1$ نحصل عليها من C بإضافة إحداثي واحد لكل من كلمات الشفرة C بحيث يُصبح وزن كل من كلمات الشفرة C^* زوجياً. تُسمى C^* **امتداداً للشفرة** C (**C^* Extended Code of C**).

أنشأنا في المثال (**١,٣,٣**) امتداداً للشفرة K^2 كما طلبنا من القارئ إنشاء امتداد للشفرة K^3 في التمرين (**١,٣,٥**).

إذا كانت درجة مصفوفة مولّدة G للشفرة الأصلية C هي $k \times n$ فمن الواضح أن :

$$G^* = [G \ \ b]$$

هي مصفوفة مولّدة للشفرة C^* وهي من الدرجة $k \times (n+1)$، حيث تمت إضافة العمود b بحيث يكون وزن كل من صفوف G^* زوجياً.

يمكن استخدام G^* والخوارزمية (**٢,٥,٧**) لإنشاء مصفوفة اختبار النوعية للشفرة C^* ولكن من الممكن إنشاء هذه المصفوفة بطريقة أسهل باستخدام مصفوفة اختبار النوعية H للشفرة C. في هذه الحالة تكون مصفوفة اختبار النوعية للشفرة الممتدة C^* هي :

$$H^* = \begin{bmatrix} H & j \\ 0 & 1 \end{bmatrix}$$

حيث j هو العمود من الدرجة $n \times 1$ الذي جميع عناصره تساوي 1. لاحظ أن درجة H^* هي $(n+1) \times (n+1-k)$. وبما أن رتبة H هي $n-k$ فيضمن لنا عمود H^* الأخير أن تكون رتبة H^* هي $n-k+1$. إضافة إلى ذلك يكون:

$$G^*H^* = [G \;\; b]\begin{bmatrix} H & j \\ 0 & 1 \end{bmatrix} = [GH \quad Gj+b]$$

وبما أن $GH = 0$ وأن Gj يجمع الإحداثيات 1 من جميع صفوف G فنجد من تعريف b أن $Gj + b = 0$. وبهذا نرى أن $G^*H^* = 0$. واستناداً إلى المبرهنة **(٢,٧,٦)** نرى أن G^* و H^* هما بالفعل مصفوفة مولّدة ومصفوفة اختبار النوعية على التوالي للشفرة C^*.

مثال (٣,٤,١)

لتكن G مصفوفة مولّدة للشفرة الخطية C:

$$G = \begin{bmatrix} 10010 \\ 01001 \\ 00111 \end{bmatrix}.$$

عندئذ، تكون:

$$H = \begin{bmatrix} 10 \\ 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

مصفوفة اختبار النوعية للشفرة C وذلك استناداً إلى الخوارزمية **(٢,٥,٧)**. وبهذا نحصل على مصفوفة مولّدة ومصفوفة اختبار النوعية للشفرة الممتدة C^* وهما:

$$G^* = \left[\begin{array}{c|c} 10010 & 0 \\ 01001 & 0 \\ 00111 & 1 \end{array}\right] \quad \text{و} \quad H^* = \left[\begin{array}{c|c} 10 & 1 \\ 01 & 1 \\ 11 & 1 \\ 10 & 1 \\ 01 & 1 \\ \hline 00 & 11 \end{array}\right]. \qquad \blacktriangle$$

إذا كانت v كلمة من كلمات الشفرة الأصلية C وكانت v^* الكلمة المقابلة في الشفرة الممتدة C^* فنجد أن:

$$wt(v^*) = \begin{cases} wt(v) & \text{، إذا كان وزن } v \text{ زوجياً} \\ wt(v)+1 & \text{، إذا كان وزن } v \text{ فردياً} \end{cases}.$$

وبهذا، إذا كانت المسافة d للشفرة C فردية فتكون مسافة C^* هي $d+1$ وأما إذا كانت المسافة d زوجية فتكون مسافة C^* هي d أيضاً. ومن ثم يكون للشفرة الممتدة فائدة في الحالة التي تكون فيها مسافة الشفرة الأصلية C فردية وفي هذه الحالة فهي تُصوّب نفس عدد أنماط الأخطاء التي تُصوبها الشفرة الأصلية ولكنها تستطيع اكتشاف نمط خطأ زيادة عن الشفرة الأصلية. لاحظ أننا لن نجني أي فائدة من تمديد الشفرة مرتين.

مثال (٣,٤,٢)

لنفرض أن مسافة C هي $d = 5$. عندئذ، تكون مسافة C^* هي $d^* = 6$. استناداً إلى المبرهنة (**١,١١,١٤**) تكتشف C جميع أنماط الأخطاء غير الصفرية ذات الأوزان التي لا تزيد عن $d - 1 = 4$ وتكتشف C^* جميع أنماط الأخطاء غير الصفرية ذات الأوزان التي لا تزيد عن $d^* - 1 = 5$. واستناداً إلى المبرهنة (**١,١٢,٩**) تُصوّب C جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $\lfloor (d-1)/2 \rfloor = \lfloor 4/2 \rfloor = 2$ وتُصوّب C^* جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $\lfloor (d^*-1)/2 \rfloor = \lfloor 5/2 \rfloor = 2$. ▲

تمارين

(**٣,٤,٣**) جد مصفوفة مولّدة ومصفوفة اختبار النوعية لشفرة هامينغ الممتدة من الطول 8.

(**٣,٤,٤**) أنشئ جدول SDA لشفرة هامينغ الممتدة من الطول 8 واستخدمها لفك تشفير الكلمات التالية:

(أ) 10101010 (ب) 11010110 (ج) 11111111.

(٣,٤,٥) أثبت أن شفرة هامينغ الممتدة من الطول 8 هي ذاتية الثنوية (أي أن $C = C^{\perp}$).

(٣,٤,٦) جد صيغة للمسافة d^* للشفرة الممتدة C^* بدلالة مسافة الشفرة الأصلية C.

(٣,٤,٧) لتكن C شفرة هامينغ من الطول 15. جد عدد أنماط الأخطاء التي تضمن لنا المبرهنة **(١,١١,١٤)** أن C^* تستطيع اكتشافها وعدد أنماط الأخطاء التي تضمن لنا المبرهنة **(١,١٢,٩)** أن C^* تستطيع تصويبها. ما هو العدد الفعلي لأنماط الأخطاء التي تُصوّبها C^* ؟

(٣,٥) شفرة غوليه الممتدة

The Extended Golay Code

نقوم في هذا البند والبندين القادمين بإنشاء شفرتين تُصوّبان ثلاثة أخطاء فأقل. شفرة غوليه الممتدة التي نناقشها في هذا البند والبند الذي يليه هي الشفرة التي استخدمت في برنامج مكُوك الفضاء **فويجر** **(Voyager)** في بدايات الثمانينيات من القرن العشرين والذي قام بإرسال الصور القريبة لكوكبي **زحل والمشتري** **(Jupiter & Saturn)**.

لنفرض أن B هي المصفوفة التالية من الدرجة 12×12 :

$$B = \begin{bmatrix}
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{bmatrix}$$

ولنفرض أن $G = [I \quad B]$ هي المصفوفة من الدرجة 12×24 حيث I المصفوفة المحايدة من الدرجة 12×12. تُسمى الشفرة الخطية C التي لها المصفوفة المولّدة G،

شفرة غوليه الممتدة (Extended Golay Code) ويُرمز لها بالرمز C_{24}. للمساعدة على تذكر المصفوفة B نفرض أن B_1 هي المصفوفة التي نحصل عليها من B بحذف الصف الأخير والعمود الأخير. عندئذ، للمصفوفة B_1 خاصية الدورية حيث الصف الأول منها هو 11011100010، ونحصل على الصف الثاني من B_1 بإزاحة كل من إحداثيات الصف الأول إلى اليسار بموقع واحد وإزاحة الإحداثي الأول ليكون الإحداثي الأخير والصف الثالث نحصل عليه من الصف الثاني بالطريقة نفسها وهكذا بقية الصفوف. وبهذا نرى أن المصفوفة B هي:

$$B = \begin{bmatrix} B_1 & j^T \\ j & 0 \end{bmatrix}$$

حيث j كلمة طولها 11 وجميع إحداثياتها تساوي 1. من الواضح أن $B^T = B$. أي أن B مصفوفة متماثلة.

نقدم الآن سبع خصائص مهمة تتمتع بها شفرة غوليه الممتدة C_{24} حيث $G = [I \quad B]$ مصفوفة مولّدة لها:

(١) C_{24} من الطول $n = 24$ والبعد $k = 12$ وعدد كلماتها يساوي $4096 = 12^{12}$. وهذا واضح من المصفوفة G.

(٢) مصفوفة اختبار النوعية للشفرة C_{24} هي المصفوفة:

$$\begin{bmatrix} B \\ I \end{bmatrix}$$

من الدرجة 24×12. ونحصل على هذه الخاصية من الخوارزمية (**٢,٥,٧**).

(٣) مصفوفة اختبار نوعية أخرى للشفرة C_{24} هي المصفوفة:

$$H = \begin{bmatrix} I \\ B \end{bmatrix}$$

من الدرجة 24×12. لبرهان ذلك لاحظ أولاً أن وزن كل صف من صفوف B فردي (7 أو 11). ومن ثم فحاصل الضرب القياسي لأي صف مع نفسه يساوي 1.

ومن السهل رؤية أن الضرب القياسي للصف الأول من المصفوفة B مع أي صف آخر يساوي 0. ومن خاصية الدورية للمصفوفة B_1 نرى أن الضرب القياسي لأي صفين مختلفين من B يساوي 0. ومن ذلك نرى أن $BB^T = I$. وبما أن $B^T = B$ فنجد أن $B^2 = BB^T = I$. وبهذا نرى أن :

$$GH = [I \;\; B]\begin{bmatrix} I \\ B \end{bmatrix} = I^2 + B^2 = I + BB^T = I + I = 0$$

سوف نستخدم كلا مصفوفتي اختبار النوعية لفك تشفير C_{24}.

(٤) مصفوفة مولّدة أخرى للشفرة C_{24} هي المصفوفة $[B \quad I]$ من الدرجة 12×24.

(٥) الشفرة C_{24} ذاتية الثنوية ، أي أن $C_{24} = C_{24}^{\perp}$.

(٦) مسافة C_{24} تساوي 8.

(٧) C_{24} تُصوّب أنماط خطأ من النوع 3.

نترك برهان الفقرتين (٤) و (٥) للتمارين. أما برهان الفقرة (٧) فينتج مباشرة من الفقرة (٦)، ولذا نبرهن الفقرة (٦) حيث يحتوي برهانها على خصائص مهمة أخرى للشفرة C_{24}. وسننجز هذا البرهان على ثلاث مراحل.

المرحلة الأولى

وزن كل من كلمات الشفرة C_{24} مضاعف للعدد 4. ولرؤية ذلك، لاحظ أولاً أن أوزان صفوف G هي إما 8 أو 12. لنفرض أن $v \in C_{24}$ حيث $v = r_i + r_j$ و r_i ، r_j صفان مختلفان من G. بما أن صفوف B متعامدة فتكون صفوف G متعامدة. وبهذا يكون عدد الإحداثيات التي قيمها 1 المشتركة بين r_i و r_j هو عدداً زوجياً وليكن $2x$. إذن :

$$wt(v) = wt(r_i) + wt(r_j) - 2(2x)$$

وهذا مضاعف للعدد 4.

نفرض الآن أن $v \in C_{24}$ هي $v = r_i + r_j + r_k$ وأن $r_i \neq r_j \neq r_k$ صفوف من G.
ولنفرض أن $v_1 = r_i + r_j$. وبما أن C_{24} ذاتية الثنوية نرى أن $v_1 \cdot r_k = 0$. وبهذا يشترك v_1 و r_k بعدد زوجي من الإحداثيات التي قيمها 1 وليكن $2y$. إذن:

$$wt(v) = wt(v_1) + wt(r_k) - 2(2y)$$

وهذا مضاعف للعدد 4. وبالاستمرار على هذا المنوال (أي باستخدام الاستقراء) نتوصل إلى أنه إذا كانت $v \in C_{24}$ تركيباً خطياً لصفوف من G فإن $wt(v)$ مضاعف للعدد 4 ونخلص إلى أن وزن أي $v \in C_{24}$ هو مضاعف للعدد 4.

المرحلة الثانية

الأحد عشر صفاً الأولى من G هي كلمات شفرة من C_{24} وزن كل منها 8. وبهذا تكون مسافة C_{24} إما 4 أو 8.

المرحلة الثالثة

سنبرهن الآن عدم وجود كلمات وزنها 4 في الشفرة C_{24}. ولهذا الغرض نفرض أن v كلمة غير صفرية من كلمات C_{24} حيث $wt(v) = 4$. بما أن كلاً من $[I \quad B]$ و $[B \quad I]$ مصفوفة مولّدة للشفرة C_{24}، فيوجد u_1 و u_2 بحيث يكون $v = u_1[I \quad B]$ و $v = u_2[B \quad I]$ و $wt(u_1) \leq 2$ و $wt(u_2) \leq 2$؛ (لأن نصف v يحتوي على الأكثر على إحداثيين من القيمة 1). ولكن لا يمكن أن يكون وزن مجموع صفين من B على الأكثر 3. إذن، $wt(u_i) + wt(u_iB) > 4$. وبهذا فلا يمكن أن يكون وزن v يساوي 4.

تمارين

(**٣,٥,١**) أثبت أن الكلمة التي جميع إحداثياتها 1 تنتمي إلى C_{24}. استنتج أن C_{24} لا تحتوي على كلمة وزنها 20.

(**٣,٥,٢**) أثبت الخاصية (٤) للشفرة C_{24}.

(٣,٥,٣) أثبت الخاصية (٥) للشفرة C_{24}.

(٣,٥,٤) استخدم المبرهنة (**٢,٩,١**) للتحقق من أن مسافة C_{24} تساوي 8.

(٣,٦) فك تشفير شفرة غوليه الممتدة
Decoding the Extended Golay Code

نقدم الآن خوارزمية لطريقة IMLD لفك تشفير الشفرة C_{24}. في هذا البند، w هي الكلمة المرسلة وv هي كلمة الشفرة الأقرب إلى w و $u = v + w$ نمط الخطأ. هدفنا هو تصويب جميع أنماط الأخطاء من الأوزان التي لا تزيد عن 3، ولذا سنفرض أن $wt(u) \leq 3$. سنضع علامة الفاصلة بين أول 12 إحداثي وآخر 12 إحداثي لكلمات K^{24} وسنكتب نمط الخطأ على الشكل $u = [u_1 , u_2]$ حيث طول كل من u_1 و u_2 يساوي 12. هدفنا هو إيجاد كلمة طليعية u للمجموعة المشاركة التي تحتوي w دون الرجوع إلى جدول SDA للشفرة C_{24}.

بما أننا افترضنا أن $wt(u) \leq 3$ فيكون $wt(u_1) \leq 1$ أو $wt(u_2) \leq 1$. لنفرض أن s_1 هي تناذُر $w = v + u$ حيث استخدمنا عند حسابها مصفوفة اختبار النوعية.

$$H = \begin{bmatrix} I \\ B \end{bmatrix}.$$

عندئذ، $s_1 = wH = [u_1 , u_2]H = u_1 + u_2B$. وبهذا نرى أنه إذا كان $wt(u_2) \leq 1$ فإما أن تكون s_1 كلمة طولها 3 على الأكثر (في الحالة $wt(u_2) = 0$) أو أن تكون صفاً من B تَغَيّر فيه إحداثيان على الأكثر (في الحالة $wt(u_2) = 1$). وبالمثل إذا كان $wt(u_1) \leq 1$. عندئذ، التناذُر:

$$s_2 = w \begin{bmatrix} B \\ I \end{bmatrix} = u_1B + u_2$$

إما أن تكون كلمة وزنها 3 على الأكثر وإما صفاً من B تغير فيه إحداثيان على الأكثر.

وبهذا نرى في كل من الحالتين أنه إذا كان وزن u على الأكثر 3 فيكون تحديدها أمراً سهلاً ؛ لأنه يمكن إيجاد 3 صفوف على الأكثر من إحدى مصفوفتي اختبار النوعية ومن ثم جمعها لنحصل على التناذر المقابل. باستخدام هذه الملحوظات والحقائق $B^2 = I$ و

$$\begin{aligned} s_1 &= u_1 + u_2 B = wH \\ s_2 &= u_1 B + u_2 \\ &= (u_1 + u_2 B)B = s_1 B \end{aligned}$$

نستطيع تقديم خوارزمية لفك التشفير للشفرة C_{24}. سنستخدم في هذه الخوارزمية مصفوفة اختبار النوعية :

$$H = \begin{bmatrix} I \\ B \end{bmatrix}$$

فقط وهذا ممكن من الحقائق المقدمة في الفقرة السابقة. وكما هي العادة، فبمجرد إيجاد u يكون فك تشفير w هو كلمة الشفرة $v = w + u$. نستخدم الرمز e_i ليكون لكلمة من الطول 12 التي تحتوي على الإحداثي 1 في الموقع i والإحداثيات 0 في المواقع الأخرى. ونرمز للصف i من المصفوفة B بالرمز b_i.

خوارزمية (٣,٦,١) [فك تشفير شفرة غوليه الممتدة]

(١) احسب التناذُر $s = wH$.

(٢) إذا كان $wt(s) \le 3$ فإن $u = [s\,, 0]$.

(٣) إذا كان $wt(s + b_i) \le 2$ حيث b_i أحد صفوف B فإن $u = [s + b_i\,, e_i]$.

(٤) احسب التناذُر الثاني sB.

(٥) إذا كان $wt(sB) \le 3$ فإن $u = [0\,, sB]$.

(٦) إذا كان $wt(sB + b_i) \le 2$ حيث b_i أحد صفوف B فإن :

$$u = [e_i\,, sB + b_i]$$

(٧) إذا لم تتمكن من تحديد u فاطلب إعادة إرسال.

يحتاج تنفيذ الخوارزمية (**٣,٦,١**) إلى حساب 26 وزناً على الأكثر أثناء عملية فك التشفير (لاحظ أنه إذا تم تحديد u في أي من خطوات الخوارزمية فإننا نتوقف ولا نحتاج لتنفيذ باقي الخطوات).

مثال (٣,٦,٢)

فُك تشفير $w = 101111101111\,,010010010010$.

الحل

التناذُر هو:

$$s = wH = 101111101111 + 001111101110$$
$$= 10000000000$$

ونرى أن وزنه يساوي 2. وبما أن $wt(s) \leq 3$ فنجد:

$$u = [s\,, 0] = 100000000001\,,000000000000$$

ومن ثم نخلص إلى أن:

$$v = w + u = 001111101110\,,010010010010$$

هي كلمة الشفرة المرسلة. ▲

بما أن $G = [I \quad B]$ مصفوفة قياسية وأنه من الممكن تشفير أي كلمة من كلمات K^{12} على أنها رسالة (بُعد C_{24} يساوي 12) فنرى أن الرسالة المرسلة هي أول 12 إحداثي من كلمة فك التشفير v. ولذا فالرسالة المرسلة في المثال (**٣,٦,٢**) هي 001111101110.

مثال (٣,٦,٣)

فُك التشفير $w = 001001001101\,,101000101000$.

الحل

التناذُر هو:

$$s = wH = 001001001101 + 111000000100 = 110001001001$$

ونرى أن وزن s يساوي 5. ننتقل الآن إلى الخطوة (٣) من الخوارزمية (**٣,٦,١**) فنجد:

$$s + b_1 = 000110001100$$
$$s + b_2 = 011111000010$$
$$s + b_3 = 101101011110$$
$$s + b_4 = 001001100100$$
$$s + b_5 = 000000010010$$

وبما أن $wt(s + b_5) \leq 2$ فنرى:

$$u = [s + b_5 , e_5] = 000000010010 , 000010000000$$

وبهذا نخلص إلى أن:

$$v = w + u = 001001011111 , 101010101000$$

هي كلمة الشفرة المرسلة. ▲

مثال (٣,٦,٤)

فُك التشفير $w = 000111000111 , 011011010000$.

الحل

التناذُر هو:

$$\begin{aligned} s = wH &= u_1 + u_2 B \\ &= 000111000111 + 101010101101 \\ &= 101101101010 \end{aligned}$$

ووزن s يساوي 7. وبتنفيذ الخطوة (٣) نجد أن $wt(s + b_i) \geq 3$ لكل صف b_i من صفوف B. ننتقل الآن إلى الخطوة (٤) ونحسب التناذُر الثاني فنجد:

$$sB = 111001111101$$

ووزن sB يساوي 9. ولذا ننتقل إلى الخطوة (٥) لنجد:

$$sB + b_1 = 001110111000$$
$$sB + b_2 = 010111110110$$
$$sB + b_3 = 100101101010$$
$$sB + b_4 = 000001010000$$

وبما أن $wt(sB + b_4) \leq 2$ فنرى أن :

$$u = [e_4 , sB + b_4] = 000100000000 , 000001010000$$

ونستنتج أن :

$$v = w + u = 000011000111 , 011010000000$$

هي كلمة الشفرة المرسلة. ▲

تمارين

(**٣,٦,٥**) للشفرة C_{24} ، جد نمط الخطأ المرجح (إذا أمكن ذلك) لكل من الكلمات w المستقبلة التالية :

(أ) 111 000 000 000 , 011 011 011 011

(ب) 111 111 000 000 , 100 011 100 111

(ج) 111 111 000 000 , 101 011 100 111

(د) 111 111 000 000 , 111 000 111 000

(هـ) 111 000 000 000 , 110 111 001 101

(و) 110 111 001 101 , 111 000 000 000

(ز) 000 111 000 111,101 000 101 101

(ح) 110 000 000 000 , 100 100 100 000

(ط) 110 101 011 101 , 111 000 000 000.

(**٣,٦,٦**) جد نمط الخطأ الأرجح لكل من الكلمات ذات التناذرات التالية :

(أ) $s_1 = 010010000000, s_2 = 011111010000$

(ب) $s_1 = 010010100101, s_2 = 001000110000$

(ج) $s_1 = 111111000101, s_2 = 111100010111$

(د) $s_1 = 111111111011, s_2 = 010010001110$

(هـ) $s_1 = 001101110110, s_2 = 111110101101$

(و) $s_1 = 010111111001, s_2 = 100010111111$.

(٣,٦,٧) إذا كان وزن s أو sB يساوي 4 فأثبت أن طريقة IMLD تطلب إعادة إرسال الكلمة.

(٣,٧) شفرة غوليه
The Golay Code

يمكن الحصول على شفرة أخرى مهمة تُصوّب أنماط الأخطاء من النوع 3 بحذف أحد إحداثيات كلمات الشفرة C_{24} (يتم حذف الإحداثي من الموقع نفسه لجميع كلمات الشفرة). سنحذف في شفرتنا هذه الإحداثي الأخير من كلمات الشفرة C_{24}.

لنفرض أن $\hat{B}$ هي المصفوفة من الدرجة 12×11 التي نحصل عليها بحذف العمود الأخير من المصفوفة B. ولنفرض أن $G = [I_{12} \quad \hat{B}]$ المصفوفة من الدرجة 12×23. تُسمى الشفرة الخطية ذات المصفوفة المولّدة G، **شفرة غوليه (Golay Code)** ويُرمز لها بالرمز C_{23}.

طول C_{23} هو $n = 23$ وبُعدها هو $k = 12$ وعدد كلماتها هو $4096 = 2^{12}$. لاحظ أن الشفرة الممتدة C_{23}^* هي بالفعل C_{24}. وبهذا تكون مسافة C_{23} هي $d = 7$ (انظر التمرين (**٣,٤,٦**)). ومن الممكن أيضاً إثبات ذلك باستخدام المبرهنة (**٣,٢,٨**) أو بأسلوب مماثل للبرهان المقدم في إثبات أن مسافة C_{24} تساوي 8.

شفرة غوليه C_{23} هي شفرة تامة (انظر المثال (**٣,٢,٤**)) وتُصوّب فقط جميع أنماط الأخطاء من الوزن 3 فأقل (انظر المبرهنة (**٣,٢,٨**)). وبهذا تكون المسافة بين أي كلمة مستقبلة w وبين كلمة شفرة واحدة فقط هي على الأكثر 3. ونرى أنه بإضافة إحداثي 0 أو1 إلى الكلمة w بحيث يكون وزن الكلمة $w0$ أو$w1$ الناتجة عن ذلك فردياً نحصل على كلمة مسافتها على الأكثر 3 من كلمة شفرة c من كلمات C_{24} (انظر التمرين (**٣,٧,١٠**)). وباستخدام الخوارزمية (**٣,٦,١**) لفك تشفير الكلمة المرسلة

لتكون كلمة الشفرة c ومن ثم حذف الإحداثي الأخير من c يؤدي إلى الحصول على أقرب كلمة شفرة من كلمات C_{23} إلى الكلمة w.

خوارزمية (٣,٧,١) [فك تشفير شفرة غوليه]

(١) جد الكلمة $w0$ أو $w1$ (أيهما ذات وزن فردي).

(٢) فُك تشفير wi ($i = 0$ أو $i = 1$) باستخدام الخوارزمية (**٣,٦,١**) لنحصل على كلمة شفرة c من كلمات C_{24}.

(٣) احذف الإحداثي الأخير من c.

عند التطبيق العملي تكون الكلمة المستقبلة w عادة كلمة شفرة ولكن wi الناتجة من الخطوة (١) لا يمكن أن تكون كلمة شفرة (لماذا ؟). إذا كانت w كلمة شفرة فإن تناذُر wi هو الصف الأخير من المصفوفة H (لماذا ؟). ويمكن التحقق من ذلك بسهولة قبل الشروع بتنفيذ الخوارزمية (**١,٦,١**).

مثال (٣,٧,٢)

فُك التشفير $w = 001001001001\,,11111110000$.

الحل

بما أن وزن w فردي فنأخذ :

$$w0 = 001001001001\,,111111100000$$

وبهذا نرى أن $s_1 = 100010111110$. ومن ثم يكون $s_1 = b_6 + e_9 + e_{12}$. ويكون فك تشفير $w0$ هو $001001000000\,,111110100000$. ونخلص إلى أن فك تشفير w هو $001001000000\,,11111010000$. ▲

تمارين

(**٣,٧,٣**) فُك تشفير كل من الكلمات المستقبلة التي تم تشفيرها باستخدام الشفرة C_{23} :

(أ) $101011100000\,,10101011011$

(ب) 101010000001 , 11011100010

(ج) 100101011000 , 11100010000

(د) 011001001001 , 01101101111.

(**٣,٧,٤**) أثبت أن مسافة C_{23} هي $d = 7$.

(**٣,٧,٥**) احسب موثوقية C_{23} عند إرسالها عبر قناة BSC باحتمال p.

(**٣,٧,٦**) أي من C_{23} و C_{24} لها موثوقية أكبر عند استخدام قناة BSC نفسها ؟

(**٣,٧,٧**) استخدم حقيقة أن كل كلمة وزنها 4 تبعد مسافة مقدارها 7 عن كلمة شفرة واحدة (لماذا ؟) لحساب عدد الكلمات ذات الوزن 7 في شفرة غوليه [**إرشاد:** لكل كلمة شفرة c، عدد الكلمات ذات الوزن 4 التي تبعد مسافة مقدارها 3 عن c هو $\binom{7}{3}$].

(**٣,٧,٨**) استخدم التمرين (**٣,٧,٧**) لإثبات أن C_{24} تحتوي بالضبط 759 كلمة شفرة من الوزن 8. [**إرشاد:** كل كلمة وزنها 5 تبعد مسافة مقدارها 3 عن كلمة شفرة واحدة فقط].

(**٣,٧,٩**) استخدم التمرين (**٣,٥,١**) والتمرين (**٣,٧,٨**) للتحقق من جدول توزيع أوزان الشفرة C_{24} التالي:

الوزن	0	4	8	12	16	20	24
عدد الكلمات	1	0	759	2576	759	0	1

(**٣,٧,١٠**) لتكن w هي الكلمة المستقبلة المشفّرة بالشفرة C_{23}. أضف إحداثي i إلى w لتكوين كلمة wi وزنها فردي. أثبت أن بُعد wi عن كلمة شفرة من كلمات C_{24} يساوي 3 [**إرشاد:** جميع أوزان كلمات C_{24} زوجية].

(٣,٨) شفرات ريد ومولر

Reed-Muller Codes

نقدم في هذا البند دراسة مختصرة لصنف مهم من الشفرات يحتوي كحالة خاصة على شفرة هامينغ الممتدة التي درسناها سابقاً (انظر أيضاً الفصل التاسع). يرمز **لشفرة ريد ومولر من الطول 2^m والدرجة r (The rth Order Reed-Muller Code of Length 2^m)** بالرمز $RM(r,m)$ حيث $0 \le r \le m$ وتُعرف استقرائياً على النحو التالي:

(١) $RM(0,m) = \{00\cdots0\,,11\cdots1\}$ و $RM(m,m) = K^{2^m}$.

(٢) $RM(r,m) = \{(x,x+y): x \in RM(r,m-1),\ \ y \in RM(r-1,m-1)\}$

حيث $0 < r < m$.

مثال (٣,٨,١)

$$RM(0,0) = \{0,1\}$$
$$RM(0,1) = \{00,11\}$$
$$RM(1,1) = K^2 = \{00,01,10,11\}$$
$$RM(0,2) = \{0000,1111\}$$
$$RM(2,2) = K^4$$
$$RM(1,2) = \{(x,x+y): x \in \{00,01,10,11\}, y \in \{00,11\}\}.$$ ▲

نقدم الآن تعريفاً استقرائياً لمصفوفة مولّدة $G(r,m)$ لشفرة $RM(r,m)$ ونستخدم هذه المصفوفة عوضاً عن الوصف المقدم في بداية البند. تُعرف $G(r,m)$ على النحو التالي:

(١) $G(0,m) = [11\cdots1]$.

(٢) لكل $0 < r < m$ تكون:

$$G(r,m) = \begin{bmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{bmatrix}.$$

(٣) $G(m,m) = \begin{bmatrix} G(m-1,m) \\ 0\cdots01 \end{bmatrix}$.

مثال (٣,٨,٢)

$G(0,1) = [1 \quad 1]$ هي مصفوفة مولّدة للشفرة $RM(0,1)$ و $G(1,1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ مصفوفة مولّدة للشفرة $RM(1,1)$. ▲

مثال (٣,٨,٣)

إذا كان $m = 2$ فنرى أن طول الشفرة هو $4 = 2^2$. والمصفوفات المولّدة عندما $r = 1,2$ هي:

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{bmatrix} = \begin{bmatrix} 11 & 11 \\ 01 & 01 \\ 00 & 11 \end{bmatrix} \text{ و } G(2,2) = \begin{bmatrix} G(1,2) \\ 0001 \end{bmatrix} = \begin{bmatrix} 1111 \\ 0101 \\ 0011 \\ 0001 \end{bmatrix}. \quad ▲$$

مثال (٣,٨,٤)

إذا كان $m = 3$ فإن $n = 2^3 = 8$ ويكون:

$$G(0,3) = [11111111]$$

$$G(3,3) = \begin{bmatrix} G(2,3) \\ 00000001 \end{bmatrix}$$

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{bmatrix} = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0000 & 1111 \end{bmatrix}$$

$$G(2,3) = \begin{bmatrix} G(2,2) & G(2,2) \\ 0 & G(1,2) \end{bmatrix}. \quad ▲$$

تمارين

(٣,٨,٥) جد المصفوفة المولّدة $G(2,3)$.

(٣,٨,٦) جد مصفوفة مولّدة $G(r,4)$ للشفرة $RM(r,4)$ والقيم $r = 0,1,2$.

من الممكن الآن توظيف التعريف الاستقرائي وطريقة البرهان بالاستقراء الرياضي لإثبات بعض الخصائص الأساسية لشفرة ريد ومولر.

مبرهنة (٣,٨,٧)

تتمتع شفرة ريد ومولر $RM(r,m)$ من الدرجة r بالخواص التالية:

(١) طولها هو $n = 2^m$.

(٢) مسافتها هي $d = 2^{m-r}$.

(٣) بُعدها هو $k = \sum_{i=0}^{r} \binom{m}{i}$.

(٤) $RM(r-1,m)$ شفرة جزئية من $RM(r,m)$ لكل $r > 0$.

(٥) الشفرة الثنوية هي $RM(m-1-r,m)$ حيث $r < m$.

البرهان

نستخدم الاستقراء الرياضي لبرهان جميع الفقرات. من الواضح أن جميع الفقرات صائبة عندما يكون $r = 0$ و $r = m$. سنترك إثبات صواب الفقرات لجميع الشفرات $RM(r,m)$ حيث $m = 1,2,3,4$ للتمارين.

سنبرهن أولاً الفقرة (٤). أي سنبرهن أن $RM(r-1,m) \subseteq RM(r,m)$. لاحظ أولاً أن:

$$G(1,m) = \begin{bmatrix} G(1,m-1) & G(1,m-1) \\ 0 & G(0,m-1) \end{bmatrix}$$

بما أن 1 هو الصف الأعلى للمصفوفة $G(1,m-1)$ فيكون المتجه (1,1) هو الصف الأعلى في المصفوفة $[G(1,m-1) \quad G(1,m-1)]$. ومن ذلك نرى أن $RM(0,m) = \{0,1\}$ مجموعة جزئية من $RM(1,m)$. وفي العموم بما أن $G(r-1,m-1)$ مصفوفة جزئية من $G(r,m-1)$ وأن $G(r-2,m-1)$ مصفوفة جزئية من $G(r-1,m-1)$ فنجد أن:

$$G(r-1,m) = \begin{bmatrix} G(r-1,m-1) & G(r-1,m-1) \\ 0 & G(r-2,m-1) \end{bmatrix}$$

مصفوفة جزئية من $G(r,m)$. وهذا يبرهن أن $RM(r-1,m)$ شفرة جزئية من $RM(r,m)$.

سنبرهن الآن الفقرة (٢) بالاستقراء الرياضي على r. بما أن:

$$RM(r,m) = \left\{(x, x+y) : x \in RM(r,m-1) \text{ و } y \in RM(r-1,m-1)\right\}$$

وأن $RM(r-1,m-1) \subseteq RM(r,m-1)$ فنرى أن $x+y \in RM(r,m-1)$. إذا كـان $x \neq y$ فنجـد باسـتخدام الاسـتقراء الرياضـي أن $wt(x+y) \geq 2^{m-1-r}$ وأن $w(x) \geq 2^{m-1-r}$ ومن هذا نجد أن:

$$wt(x, x+y) = wt(x+y) + wt(x) \geq 2 + 2^{m-1-r} = 2^{m-r}.$$

وإذا كان $x = y$ فيكون $(x, x+y) = (0, y)$. ولأن $y \in RM(r-1, m-1)$ نجد أن:

$$wt(0,y) = wt(y) \geq 2^{m-1-(r-1)} = 2^{m-r}$$

وبهذا تنتهي خطوة الاستقراء ونخلص إلى أن $d = 2^{m-r}$.

ولبرهان الفقرة (٣) لاحظ أنه من تعريف $G(r,m)$ والاستقراء الرياضي يكون:

$$\begin{aligned} dimRM(r,m) &= dimRM(r,m-1) + dimRM(r-1,m-1) \\ &= \sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} \\ &= \sum_{i=0}^{r} \left(\binom{m-1}{i} + \binom{m-1}{i-1} \right) + \binom{m-1}{0} \end{aligned}$$

وبما أن $\binom{m-1}{0} = 1 = \binom{m}{0}$ وأن $\binom{m}{i} = \binom{m-1}{i} + \binom{m-1}{i-1}$ فيكون:

$$dimRM(r,m) = \sum_{i=0}^{r} \binom{m}{i} \quad .$$

ولبرهان الفقرة (٥) افرض أن:

$$RM(r,m) = \{(x, x+y) : x \in RM(r,m-1), y \in RM(r-1,m-1)\}$$

وأن:

$$\begin{aligned} RM(m-r-1,m) = \{(x', x'+y' : x' \in RM(m-r-1,m-1), \\ y' \in RM(m-r-2,m-1)\} \end{aligned}$$

وباستخدام فرضية الاستقراء فإن الشفرة الثنوية للشفرة $RM(r,m-1)$ هي $RM(m-r-2,m-1)$ وأن الشفرة الثنوية للشفرة $RM(r-1,m-1)$ هي $RM(m-r-1,m-1)$. وبهذا نجد أن $x\cdot y'=0$ وأن $x'\cdot y=0$.

أيضاً، بما أن $y\cdot y'=0$ وأن $RM(r-1,m-1)\subseteq RM(r,m-1)$ نجد أن:

$$\begin{aligned}(x,x+y)\cdot(x',x'+y') &= (x+y)\cdot(x'+y')+x\cdot x'\\ &= 2(x\cdot x')+x\cdot y'+y\cdot x'+y\cdot y'=0\end{aligned}$$

وبهذا تكون كل متجهات الشفرة $RM(r,m)$ عمودية على كل من متجهات الشفرة $RM(m-r-1,m)$. وبما أن:

$$\begin{aligned}dimRM(r,m)+dimRM(m-r-1,m) &= \sum_{i=0}^{r}\binom{m}{i}+\sum_{i=0}^{m-r-1}\binom{m}{i}\\ &= \sum_{i=0}^{r}\binom{m}{m-i}+\sum_{j=0}^{m-r-1}\binom{m}{j}\\ &= \sum_{j=0}^{m}\binom{m}{j}=2^m\end{aligned}$$

فنستنتج أن $RM(m-r-1,m)$ هي الشفرة الثنوية للشفرة $RM(r,m)$. ■

تمرين

(**٣,٨,٨**) أثبت صواب فقرات المبرهنة (**٣,٨,٧**) للشفرة $RM(r,m)$ حيث $1\le m\le 4$ مُستعيناً بالأمثلة (**٣,٨,١**)، (**٣,٨,٣**)، (**٣,٨,٤**) والتمرينين (**٣,٨,٥**) و (**٣,٨,٦**).

نقوم الآن بفك تشفير شفرة ريد ومولر الخاصة $RM(1,m)$ التي هي من الدرجة 1. لاحظ أن بُعد $RM(m-2,m)$ هو 2^m-m-1 وأن مسافتها هي 4 وطولها هو 2^m. وبهذا تكون هذه الشفرة هي شفرة هامينغ الممتدة. واستناداً إلى المبرهنة (**٣,٨,٧**) تكون $RM(1,m)$ هي الشفرة الثنوية لشفرة هامينغ الممتدة $RM(m-2,m)$. نقدم الآن خوارزمية

فعّالة لفك تشفير هذه الشفرة ونؤجل فك تشفير الشفرة العامة $RM(r,m)$ إلى الفصل التاسع.

لاحظ أن $RM(1,m)$ شفرة صغيرة مسافتها كبيرة ومن الممكن إنجاز هذه الخوارزمية بفعالية جيدة، وخوارزمية فك تشفيرها هي الخوارزمية البدائية التالية:

لكل كلمة مستقبلة w جد كلمة شفرة من $RM(1,m)$ الأقرب إلى w.

مثال (٣,٨,٩)

لنأخذ الشفرة $RM(1,3)$ حيث $m = 3$. طولها هو $2^3 = 8$ وعدد كلماتها $2^{3+1} = 16$.

مسافتها تساوي 4 ومصفوفة مولّدة لها هي:

$$G(1,3) = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0000 & 1111 \end{bmatrix}.$$

إذا استقبلنا w وكان $d(w,c) < 2$ فيكون فك تشفير w هو c. أما إذا كان $d(w,c) > 6$ فنرى أن $d(w,1+c) < 2$ ومن ثم يكون فك تشفير w هو $c + 1$ (تذكر أن 1 هي كلمة شفرة). فمثلاً إذا كانت $w = 10001111$ هي الكلمة المستقبلة فتكون $c = 00001111$ هي كلمة الشفرة الأقرب. أما إذا كانت $w = 10101011$ هي الكلمة المستقبلة فنجد أن $c = 01010101$ حيث $d(w,c) > 6$ ومن ثم تكون $c + 1 = 10101010$ هي كلمة الشفرة الأقرب. نرى مما سبق أننا نحتاج لاختبار نصف كلمات $RM(1,m)$ على الأكثر. في الحقيقة، توجد طرائق مصفوفية فعالة لحساب هذه المسافات وسنقدمها في البند التالي. ▲

تمارين

(**٣,٨,١٠**) لتكن $G(1,3)$ مصفوفة مولّدة للشفرة $RM(1,3)$. فك تشفير كل من الكلمات المستقبلة التالية:

(أ) 01011110 (ب) 01100111

(ج) 00010100 (د) 11001110.

(**٣,٨,١١**) لتكن $G(1,4)$ مصفوفة مولّدة للشفرة $RM(1,4)$. فُك تشفير كل من الكلمات المستقبلة التالية:

(أ) 1011011001101001 (ب) 1111000001011111.

(٣,٩) فك تشفير سريع للشفرة $RM(1,m)$

Fast Decoding for $RM(1,m)$

نقدم في هذا البند باختصار وبدون تبرير طريقة فعّالة جداً لفك تشفير الشفرات $RM(1,m)$. نوظف لهذه الطريقة **تحويل هادامار السريع (Fast Hadamard Transform)** لإيجاد أقرب كلمة شفرة. ونحتاج أولاً إلى **ضرب كرونكر (Kronecker Product)** للمصفوفات المعرف على النحو $A \times B = [a_{ij}B]$. أي، نقوم باستبدال العنصر a_{ij} من A بالمصفوفة $a_{ij}B$.

مثال (٣,٩,١)

إذا كانت $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ و $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ فيكون:

$$I_2 \times H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

و

$$H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}.$$ ▲

نعرّف الآن متتالية من المصفوفات على النحو التالي:

$H_m^i = I_{2^{m-i}} \times H \times I_{2^{i-1}}$ حيث $i = 1,2,\cdots,m$ و H المصفوفة المقدمة في المثال (**٣,٩,١**).

مثال (٣,٩,٢)

إذا كان $m = 2$ فإن :

$$H_2^1 = I_2 \times H \times I_1 = I_2 \times H$$

$$.H_2^2 = I_1 \times H \times I_2 = H \times I_2$$ ▲

مثال (٣,٩,٣)

إذا كان $m = 3$ فإن :

$$H_3^1 = I_4 \times H \times I_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H_3^2 = I_2 \times H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

$$H_3^3 = H \times I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

تقترح الطريقة الاستقرائية التي استخدمت لإنشاء الشفرة $RM(1,m)$ وجود طريقة استقرائية لفك التشفير وهذه هي الفكرة الأساسية المبنية عليها خوارزمية فك تشفير $RM(1,m)$ التالية :

خوارزمية (٣,٩,٤) [فك تشفير الشفرة $RM(1,m)$]

لنفرض أن w كلمة مستقبلة وأن $G(1,m)$ مصفوفة مولّدة للشفرة $RM(1,m)$.

(١) كوّن الكلمة $\overline{w}$ من w باستبدال الإحداثيات 0 بإحداثيات -1.

(٢) احسب $w_1 = \overline{w}H_m^1$ و $w_i = w_{i-1}H_m^i$ لكل $i = 2,3,\cdots,m$.

(٣) جد الموقع j في الكلمة w_m للإحداثي الذي قيمته المطلقة أكبر ما يمكن.

لنفرض أن $v(j) \in K^m$ هو التمثيل الثنائي للعدد j (يبدأ من اليسار بالإحداثي ذي القوة الأصغر). عندئذ، إذا كان الإحداثي في الموقع j من w_m موجباً فتكون الرسالة المفترضة هي $(1, v(j))$ أما إذا كان سالباً فتكون الرسالة المفترضة هي $(0, v(j))$.

مثال (٣,٩,٥)

لنفرض أن $m = 3$ وأن $G(1,3)$ هي مصفوفة مولّدة للشفرة $RM(1,3)$ (انظر التمرين (٣,٩,٨)). إذا كانت $w = 10101011$ الكلمة المستقبلة فتكون $\overline{w} = (1,-1,1,-1,1,-1,1,1)$. نقوم الآن بحساب :

$$w_1 = \overline{w}H_3^1 = (0,2,0,2,0,2,2,0)$$
$$w_2 = w_1H_3^2 = (0,4,0,0,2,2,-2,2)$$
$$w_3 = w_2H_3^3 = (2,6,-2,2,-2,2,2,-2)$$

(انظر المثال (٣,٩,٢) لقيم H_3^1 ، H_3^2 ، H_3^3). أكبر قيمة في w_3 هي القيمة 6 في الموقع الأول. وبما أن $v(1) = 100$ و $6 > 0$ فتكون الرسالة المفترضة هي $m = (1101)$.

لنفرض الآن أن $w = (10001111)$. عندئذ، تكون $\overline{w} = (1,-1,-1,-1,1,1,1,1)$ ويكون :

$$w_1 = \overline{w}H_3^1 = (0,2,-2,0,2,0,2,0)$$

$$w_2 = w_1 H_3^2 = (-2,2,2,2,4,0,0,0)$$
$$w_3 = w_2 H_3^2 = (2,2,2,2,-6,2,2,2)$$

الإحداثي الأكبر في w_3 هو 6− وهو في الموقع 4. وبما أن $v(4) = 001$ وأن $-6 < 0$ فتكون الرسالة المفترضة هي (0001). ▲

تمارين

(٣,٩,٦) فُك تشفير الكلمات المستقبلة المقدمة في التمرين **(٣,٨,١٠)** باستخدام الخوارزمية **(٣,٩,٤)** والمثال **(٣,٩,٢)**.

(٣,٩,٧) احسب H_4^i لكل من $i = 1,2,3,4$.

(٣,٩,٨) فُك تشفير الكلمات المستقبلة المقدمة في التمرين **(٣,٨,١١)** باستخدام الخوارزمية **(٣,٩,٤)** والتمرين **(٣,٩,٦)**.

الفصل الرابع

الشفرات الخطية الدورية
Cyclic Linear Codes

(٤,١) كثيرات الحدود والكلمات
Polynomials & Words

سيكون من الملائم تمثيل الشفرات الدورية بدلالة كثيرات الحدود. ولهذا الغرض نبدأ بمراجعة الحقائق التي نحتاجها عن كثيرات الحدود بمتغير واحد.

كثيرة الحدود من الدرجة n على K هي $a_0 + a_1x + \cdots + a_nx^n$ حيث المعاملات $a_0, a_1, \cdots, a_n$ عناصر تنتمي إلى K. يُرمز لمجموعة كثيرات الحدود على K بالرمز $K[x]$. كما يرمز لكثيرات الحدود (عناصر $K[x]$) بالرموز $f(x)$ ، $g(x)$ ، $p(x)$ وهكذا ويُرمز لدرجة كثيرة الحدود $f(x)$ بالرمز $deg(f(x))$.

عمليتا جمع وضرب كثيرات الحدود على K هما كالمعتاد مع ملاحظة أن $1 + 1 = 0$. أي أن $x^k + x^k = 0$ ومن ثم ليس بالضرورة أن تتحقق المساواة:

$$deg\big(f(x) + g(x)\big) = max\{deg\big(f(x)\big), deg(g(x))\}.$$

مثال (٤,١,١)

إذا كان $f(x) = 1 + x + x^3 + x^4$ ، $g(x) = x + x^2 + x^3$ ، $h(x) = 1 + x^2 + x^4$ فنجد أن:

(أ) $f(x) + g(x) = 1 + x^2 + x^4$.

(ب) $f(x) + h(x) = x + x^2 + x^3$.

(ج) $f(x)g(x) = (x + x^2 + x^3) + x(x + x^2 + x^3) +$
$x^3(x + x^2 + x^3) + x^4(x + x^2 + x^3) = x + x^7$

▲

تمارين

(٤,١,٢) جد مجموع وحاصل ضرب كل زوج من أزواج كثيرات الحدود التالية على K:

(أ) $f(x) = x^5 + x^6 + x^7 \ , h(x) = 1 + x^2 + x^3 + x^4$.

(ب) $f(x) = 1 + x^2 + x^3 + x^8 + x^{13} \ , h(x) = 1 + x^3 + x^9$.

(ج) $f(x) = 1 + x \ , h(x) = 1 + x + x^2 + x^3 + x^4$.

(٤,١,٣) إذا كانت $f(x) = 1 + x$ فجد:

(أ) $(f(x))^2$ (ب) $(f(x))^3$ (ج) $(f(x))^4$.

(٤,١,٤) أعد التمرين **(٤,١,٣)** لكثيرة الحدود $f(x) = 1 + x + x^2$.

(٤,١,٥) جد جميع كثيرات الحدود على K من الدرجة n حيث $n = 0,2,3,4$.

(٤,١,٦) جد عدد كثيرات الحدود على K ذات الدرجات التي لا تزيد عن 10.

(٤,١,٧) لقد لاحظت في التمرينين **(٤,١,٣)** (أ) و **(٤,١,٤)** (أ) أن $(f(x) + g(x))^2 = (f(x))^2 + (g(x))^2$ لأي كثيرتي حدود $f(x)$ و $g(x)$ على K؛ وذلك لأن $x^k + x^k = 0$. هل تستطيع إيجاد صيغة خاصة لحساب كل من:

(أ) $(f(x) + g(x))^4$ (ب) $(f(x) + g(x))^3$

(ج) $(f(x) + g(x))^n$ حيث n عدد صحيح موجب.

عملية القسمة المطوّلة لكثيرات الحدود على K مشابهة تماماً لعملية القسمة المطوّلة لكثيرات الحدود على الأعداد الكسرية.

خوارزمية (٤,١,٨) [خوارزمية القسمة Division Algorithm]

لتكن $f(x), h(x) \epsilon K[x]$ حيث $h(x) \neq 0$. عندئذ، توجد كثيرتا حدود وحيدتان $q(x), r(x) \epsilon K[x]$ تحققان:

$$f(x) = q(x)h(x) + r(x)$$

حيث $r(x) = 0$ أو $deg(r(x)) < deg(h(x))$.

تُدعى كثيرة الحدود $q(x)$ **خارج القسمة (quotient)** وتُدعى كثيرة الحدود $r(x)$ **باقي القسمة (remainder)**. تجرى قسمة $f(x)$ على $h(x)$ بعملية القسمة المطوّلة المعتادة مع ملاحظة أن المعاملات تنتمي إلى K.

مثال (٤,١,٩)

إذا كانت $f(x) = x + x^2 + x^6 + x^7 + x^8$ وكانت $h(x) = 1 + x + x^2 + x^4$ فيكون:

$$x^4 + x^3$$
$$x^4 + x^2 + x + 1 \;\big|\; x^8 + x^7 + x^6 + x^2 + x$$
$$x^8 + x^6 + x^5 + x^4$$
$$x^7 + x^5 + x^4 + x^2 + x$$
$$x^7 + x^5 + x^4 + x^3$$
$$x^3 + x^2 + x$$

وبهذا نرى أن خارج القسمة هو $q(x) = x^3 + x^4$ وباقي القسمة هو $r(x) = x + x^2 + x^3$. لاحظ أنه من الممكن التعبير عن ذلك بكتابة:

$$f(x) = h(x)(x^3 + x^4) + (x + x^2 + x^3)$$

لاحظ أيضاً أن $deg(r(x)) < deg(h(x))$. ▲

تمارين

(**٤,١,١٠**) جد خارج القسمة والباقي عند قسمة $f(x)$ على $h(x)$ لكثيرات الحدود على K المقدمة في التمرين (**٤,١,٢**).

(**٤,١,١١**) جد خارج القسمة والباقي عند قسمة $f(x)$ على $h(x)$ لكثيرات الحدود التالية:

(أ) $.f(x) = x^2 + x^3 + x^4 + x^8 \, , h(x) = 1 + x^5$

(ب) $.f(x) = 1 + x^{10} \, , h(x) = 1 + x^5$

(ج) $.f(x) = 1 + x^7 \, , h(x) = 1 + x + x^3$

(د) $.f(x) = 1 + x^{15} \, , h(x) = 1 + x^4 + x^6 + x^7 + x^8$

يمكن تمثيل كثيرة الحدود $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ التي درجتها لا تزيد عن $n-1$ على K ككلمة $v = a_0a_1a_2 \cdots a_{n-1}$ من الطول n في K^n. على سبيل المثال إذا كان $n = 7$ فإن:

الكلمة	كثيرة الحدود
1110100	$1 + x + x^2 + x^4$
1000111	$1 + x^4 + x^5 + x^6$
1101000	$1 + x + x^3$

وعليه يمكن تمثيل شفرة C طولها n كمجموعة كثيرات حدود على K درجاتها لا تزيد عن $n-1$. أي أنه يوجد تقابل بين كثيرات الحدود على K التي لا تزيد درجاتها عن $n-1$ والكلمات من الطول n في K^n.

عند تمثيل الكلمات بكثيرات الحدود يكون من المناسب ترقيم إحداثيات الكلمة التي طولها n من 0 إلى $n-1$ عوضاً عن الترقيم من 1 إلى n. فالكلمة $a_0a_1a_2a_3$ ذات الطول 4 تمثل بكثيرة الحدود $a_0 + a_1x + a_2x^2 + a_3x^3$ من الدرجة الثالثة.

مثال (٤,١,١٢)

العمود الأيسر من الجدول التالي يُبيّن كلمات شفرة C والعمود الأيمن يُبيّن كثيرات الحدود المقابلة لهذه الكلمات.

كثيرة الحدود $c(x)$	كلمة الشفرة
0	0000
$1+x^2$	1010
$x+x^3$	0101
$1+x+x^2+x^3$	1111 ▲

تمارين

(**٤,١,١٣**) مثّل كلاً من الشفرات C التالية بمجموعة كثيرات حدود:

(أ) $C=\{000,001,010,011\}$.

(ب) $C=\{00000,11111\}$.

(ج) $C=\{0000,0001,1110\}$.

(د) $C=\{0000,1001,0110,1111\}$.

(هـ) $C=\{00000,11100,00111,11011\}$.

(**٤,١,١٤**) اكتب كلمات شفرة هامينغ من الطول 7 ذات المصفوفة المولّدة G المعطاة، ثم مثّل هذه الكلمات بكثيرات حدود:

$$G=\begin{bmatrix}1000111\\0100110\\0010101\\0001011\end{bmatrix}.$$

وجدنا في التمرين (**٤,١,١١**) (أ) أن باقي قسمة $f(x)=x^2+x^3+x^4+x^8$ على $h(x)=1+x^5$ هو $r(x)=x^2+x^4$. لاحظ أن هذا الباقي وحيد ودرجته أصغر من درجة $h(x)$.

نقول إن $\boldsymbol{f(x)}$ **قياس** $\boldsymbol{h(x)}$ ($\boldsymbol{f(x)}$ **modulo** $\boldsymbol{h(x)}$) هي $\boldsymbol{r(x)}$ إذا كانت $\boldsymbol{r(x)}$ هي **باقي قسمة** $\boldsymbol{f(x)}$ **على** $\boldsymbol{h(x)}$ ونكتب $\boldsymbol{r(x)\equiv f(x)(mod\ h(x))}$. كما نقول إن $f(x)$ و $p(x)$ متكافئتان قياس $h(x)$ إذا وفقط إذا كان لهما الباقي نفسه عند قسمتهما على $h(x)$. أي أن:

$$f(x)\big(mod\ h(x)\big)\equiv r(x)\equiv p(x)(mod\ h(x)).$$

وفي هذه الحالة نكتب $f(x) \equiv p(x)(mod\ h(x))$[١].

مثال (٤,١,١٥)

افرض أن $h(x) = 1 + x^5$ وأن $f(x) = 1 + x^4 + x^9 + x^{11}$. بقسمة $f(x)$ على $h(x)$ نحصل على الباقي $r(x) = 1 + x$. وبالمثل إذا كانت $p(x) = 1 + x^6$ فنجد أن $1 + x^6 \equiv 1 + x(mod\ h(x))$ ويكون $p(x) \equiv f(x)(mod\ h(x))$. ▲

مثال (٤,١,١٦)

لتكن $h(x) = 1 + x^2 + x^5$. بحساب $f(x)(mod\ h(x))$ حيث $f(x) = 1 + x^2 + x^6 + x^9 + x^{11}$ نجد أن الباقي هو $r(x) = x + x^4$. وبهذا نرى أن $x + x^4 \equiv f(x)(mod\ h(x))$. وإذا كانت $p(x) = x^2 + x^8$ فنجد أن $p(x)(mod\ h(x)) \equiv 1 + x^3$. وعليه فإن $p(x)$ و $f(x)$ غير متكافئتين قياس $h(x)$. ▲

تُحافظ عمليتا جمع وضرب كثيرات الحدود على تكافؤ كثيرات الحدود. أي أن:

تمهيدية (٤,١,١٧)

إذا كانت $f(x) \equiv g(x)(mod\ h(x))$ وكانت $p(x)$ كثيرة حدود على K فإن:

$$f(x) + p(x) \equiv g(x) + p(x)(mod\ h(x))$$

$$f(x)p(x) \equiv g(x)p(x)(mod\ h(x))$$

البرهان

لنفرض أن $r(x) \equiv f(x)(mod\ h(x)) \equiv g(x)(mod\ h(x))$

وأن $s(x) \equiv p(x)(mod\ h(x))$. حينئذ،

$$\begin{aligned} f(x) + p(x) &= q_1(x)h(x) + r(x) + q_2(x)h(x) + s(x) \\ &= (q_1(x) + q_2(x))h(x) + r(x) + s(x) \end{aligned}$$

---

(١) المترجمان: استخدم المؤلفون الرمز $r(x) = f(x)\ (mod\ h(x))$ للدلالة على باقي قسمة $f(x)$ على $h(x)$ كما استخدموا الرمز $f(x) \equiv p(x)\ (mod\ h(x))$ للدلالة على أن باقي قسمة $f(x)$ على $h(x)$ يساوي باقي قسمة $p(x)$ على $h(x)$. وسنستخدم في الترجمة الرمز ≡ ليدل على الحالتين حيث يكون من الواضح المقصود من السياق وحيث أن هو الترميز الشائع الاستخدام.

وبما أن $deg(r(x)+s(x)) < deg(h(x))$ فنجد أن $r(x)+s(x) \equiv f(x) + p(x)(mod\ h(x))$. وبصورة مشابهة نجد أيضاً أن:

$$r(x)+s(x) \equiv g(x)+p(x)(mod\ h(x)).$$

الفقرة الثانية من البرهان نتركها للتمرين (**٤,١,٢٢**). ■

مثال (٤,١,١٨)

لتكن $h(x) = 1 + x^5$ و $f(x) = 1 + x + x^7$ و $g(x) = 1 + x + x^2$ و $p(x) = 1 + x^6$. لاحظ أن $f(x) \equiv g(x)(mod\ h(x))$. الآن:

$$f(x) + p(x) = x + x^6 + x^7$$
$$g(x) + p(x) = x + x^2 + x^6$$

ولكن $x + x^6 + x^7(mod\ h(x)) \equiv x^2 \equiv (x + x^2 + x^6)(mod\ h(x))$. وبالمثل

$$(1 + x + x^7)(1 + x^6)(mod\ h(x)) \equiv 1 + x^3 \equiv (1 + x + x^2)(1 + x^6)(mod\ h(x))$$

ولكن $1 + x \equiv 1 + x^6(mod\ h(x))$. من ذلك نجد أن:

$$\begin{aligned}(1 + x + x^7)(1 + x^6) &\equiv (1 + x + x^2)(1 + x^6)\\ &\equiv (1 + x + x^2)(1 + x)\\ &\equiv 1 + x^3(mod\ h(x))\end{aligned}$$ ▲

تمارين

(**٤,١,١٩**) لتكن $h(x) = 1 + x^3 + x^5$. احسب $f(x)(mod\ h(x))$ والكلمة المقابلة لها لكل مما يلي:

(أ) $f(x) = 1 + x + x^6$.

(ب) $f(x) = x + x^4 + x^7 + x^8$.

(ج) $f(x) = 1 + x^{10}$.

(**٤,١,٢٠**) افرض أن $h(x) = 1 + x^7$ احسب كلاً من $f(x)(mod\ h(x))$ و $p(x)(mod\ h(x))$ وبيّن ما إذا كان $f(x) \equiv p(x)(mod\ h(x))$:

(أ) $f(x) = 1 + x^3 + x^8$ و $p(x) = x + x^3 + x^7$.

(ب) $f(x) = x + x^5 + x^9$ و $p(x) = x + x^5 + x^6 + x^{13}$.

(ج) $f(x) = 1 + x$ و $p(x) = x + x^7$.

(**٤,١,٢١**) إذا كانت $h(x) = 1 + x^7$ فاحسب $f(x) + g(x)(mod\ h(x))$ و $f(x)g(x)(mod\ h(x))$ لما يلي :

(أ) $f(x) = 1 + x^6 + x^8$ و $g(x) = 1 + x$.

(ب) $f(x) = x + x^5 + x^9$ و $g(x) = x + x^2 + x^7$.

(ج) $f(x) = 1 + x^4 + x^5$ و $g(x) = 1 + x + x^2$.

(**٤,١,٢٢**) إذا كان $f(x) \equiv g(x)(mod\ h(x))$ فأثبت أن :

$f(x)p(x) \equiv g(x)p(x)(mod\ h(x))$.

(٤,٢) مقدمة للشفرات الدورية
Introduction to Cyclic Codes

نبدأ الآن بدراسة صنف من الشفرات تُدعى الشفرات الدورية ونستخدم لاحقاً خواص هذه الشفرات لإنشاء مصفوفة مولّدة لشفرة BCH التي تصوّب خطأين إضافة إلى بعض الشفرات الأخرى. في الحقيقة سنرى أن كلاً من شفرة هامينغ وشفرة جولاي دورية أو تكافئ شفرة دورية.

لتكن v كلمة طولها n. **الإزاحة الدورية (Cyclic Shift)** $\pi(v)$ للكلمة v هي الكلمة من الطول n التي نحصل عليها من الكلمة v بنقل الإحداثي الأخير من v إلى بداية الكلمة ثم إزاحة الإحداثيات الأخرى إلى اليمين موقعاً واحداً. على سبيل المثال :

v	10110	111000	0000	1011
$\pi(v)$	01011	011100	0000	1101

نقول إن الشفرة C هي **شفرة دورية (Cyclic Code)** إذا كانت الإزاحة الدورية لكل كلمة شفرة هي أيضاً كلمة شفرة. أي أن C مغلقة تحت تأثير الإزاحة الدورية.

مثال (٤,٢,١)

لتكن $C = \{000\,,110\,,101\,,011\}$. عندئذ الشفرة C خطية (لماذا ؟). بحساب $\pi(v)$ لكل $v\epsilon C$ نجد أن $\pi(000) = 000, \pi(110) = 011, \pi(101) = 110, \pi(011) = 101$. وبهذا نرى أن $\pi(v)\epsilon C$ لكل $v\epsilon C$. وعليه فإن C شفرة دورية وتكون C شفرة خطية دورية. ▲

مثال (٤,٢,٢)

الشفرة $C = \{000{,}100{,}011{,}111\}$ ليست دورية ؛ لأن $\pi(100) = 010 \notin C$. ▲

لاحظ أن الإزاحة الدورية π هي تحويل خطي. أي أن :

تمهيدية (٤,٢,٣)

$\pi(v+w) = \pi(v) + \pi(w)$ و $\pi(av) = a\pi(v)$ لكل $a\epsilon K = \{0,1\}$. وعليه، إذا كانت C شفرة خطية فلإثبات أن C شفرة دورية يكفي أن نثبت أن $\pi(v)\ \epsilon C$ لكل كلمة v من كلمات أساس للشفرة C.

البرهان

لنفرض أن $v = (v_0, v_1, \cdots, v_{n-1})$ وأن $w = (w_0, w_1, \cdots, w_{n-1})$. حينئذ،

$v + w = (v_0 + w_0, v_1 + w_1, \cdots, v_{n-1} + w_{n-1})$ ويكون

$$\pi(v+w) = (v_{n-1} + w_{n-1}, v_0 + w_0, \cdots, v_{n-2} + w_{n-2})$$
$$= (v_{n-1}, v_0, \cdots, v_{n-2}) + (w_{n-1}, w_0, \cdots, w_{n-2})$$
$$= \pi(v) + \pi(w)$$

أيضاً $av = (av_0, av_1, \cdots, av_{n-1})$ ويكون :

$\pi(av) = (av_{n-1}, av_0, \cdots, av_{n-2}) = a(v_{n-1}, v_0, \cdots, v_{n-2}) = a\pi(v)$.[٢] ■

---

(٢) المترجمان : أضفنا برهان الفقرة الأخيرة من التمهيدية (٤,٢,٣) نعتقد أنه سقط سهواً من الأصل الإنجليزي.

مثال (٤,٢,٤)

لاحظ أن $\{110, 101\}$ أساس للشفرة C المقدمة في المثال (**٤,٢,١**). بما أن $\pi(110) = 011 \epsilon C$ وأن $\pi(101) = 110 \epsilon C$ فتكون C شفرة خطية دورية. ▲

لإنشاء شفرة خطية دورية نقوم باختيار كلمة v ثم نجد المجموعة S المكوّنة من v وجميع إزاحاتها الدورية. أي نجد $S = \{v, \pi(v), \pi^2(v), \cdots, \pi^{n-1}(v)\}$[٣]. حينئذ. نأخذ $C = \langle S \rangle$ الشفرة المولّدة بالمجموعة S. بما أن S تحتوي على أساس للشفرة C فاستناداً إلى التمهيدية (**٤,٢,٣**) تكون C دورية. ومن ثم فهي الشفرة الخطية الدورية المنشودة.

مثال (٤,٢,٥)

لنفرض أن $n = 3$ وأن $v = 100$. عندئذ،

$$S = \{v, \pi(v), \pi^2(v)\} = \{100, 010, 001\}.$$

ومن ثم فإن $\langle S \rangle = K^3$. لاحظ أنه إذا كان $w = a_0 v + a_1 \pi(v) + a_2 \pi^3(v)$ فنرى أن:

$$\pi(w) = a_0 \pi(v) + a_1 \pi^2(v) + a_2 \pi^3(v) = a_2 v + a_0 \pi(v) + a_1 \pi^2(v).$$

▲

مثال (٤,٢,٦)

لنفرض أن $n = 4$ وأن $v = 0101$. حينئذ، $\pi(v) = 1010$ ، $\pi^2(v) = 0101$. ونرى أن $S = \{0101, 1010\}$. وبهذا تكون الشفرة الدورية $C = \langle S \rangle$ هي:

$$C = \{0000, 0101, 1010, 1111\}.$$ ▲

لتكن v كلمة ولتكن $S = \{v, \pi(v), \cdots, \pi^{n-1}(v)\}$ مجموعة الازاحات الدورية للكلمة v ولتكن $C = \langle S \rangle$ الشفرة المولّدة بالمجموعة S. حينئذ، نقول إن الكلمة v **مولّدة (generator)** للشفرة الخطية الدورية C. وبما أن أي شفرة خطية دورية تحتوي v يجب أن

---

(٣) لاحظ أن $\pi^2(v) = \pi(\pi(v))$ وأن $\pi^3(v) = \pi(\pi(\pi(v)))$ وهكذا.

تحتوي S فتكون C هي أصغر شفرة خطية دورية تحتوي v. لاحظ إمكانية وجود أكثر من مولّدة للشفرة الخطية الدورية.

تمارين

(**٤,٢,٧**) جد أساساً لأصغر شفرة خطية دورية من الطول n تحتوي v لكل من:

(أ) $v = 1101000$ ، $n = 7$.

(ب) $v = 010101$ ، $n = 6$.

(ج) $v = 11011000$ ، $n = 8$.

(**٤,٢,٨**) جد جميع الكلمات v من الطول n التي تحقق $\pi(v) = v$.

(**٤,٢,٩**) جد جميع الكلمات v من الطول 6 التي تحقق:

(أ) $\pi^2(v) = v$ (ب) $\pi^3(v) = v$.

من الممكن استخدام كثيرات الحدود للحصول على تمثيل ملائم للشفرات الدورية، وذلك بملاحظة أنه إذا كانت $v(x)$ هي كثيرة الحدود المقابلة للكلمة v فإن كثيرة الحدود $xv(x)(mod 1 + x^n)$ هي كثيرة الحدود التي تقابل الإزاحة الدورية $\pi(v)$. لاحظ أن $1 \equiv x^n(mod\ 1 + x^n)$.

مثال (٤,٢,١٠)

لنفرض أن $v = 100$. عندئذ، $v(x) = 1$ وبهذا نرى أن $\pi(v) = 010$ تقابل $xv(x) = x$. وإذا كانت $v = 1101$ فإن $v(x) = 1 + x + x^3$ وإن $\pi(v) = 1110$ تقابل $xv(x)(mod 1 + x^4) = 1 + x + x^2$. ▲

مما سبق يكون من المناسب أيضاً النظر إلى كلمات الشفرة الدورية على أنها كثيرات حدود. ولهذا، إذا كانت v كلمة طولها n وكانت $v(x)$ كثيرة الحدود المقابلة لها فإن الإزاحات الدورية للكلمة v تقابل كثيرات الحدود $x^i v(x)(mod 1 + x^n)$ حيث $i = 0,1,\cdots,n-1$.

مثال (٤,٢,١١)

لنفرض أن $v = 1101000$ وأن $n = 7$. حينئذ، $v(x) = 1 + x + x^3$ والجدول (٤,١) يُبيّن $x^i v(x)$ حيث $1 \le i \le 6$.

الجدول (٤,١). كثيرات الحدود المقابلة للإزاحات الدورية.

$x^i v(x)\ (mod\ 1 + x^7)$	الكلمة
$xv(x) = x + x^2 + x^4$	0110100
$x^2 v(x) = x^2 + x^3 + x^5$	0011010
$x^3 v(x) = x^3 + x^4 + x^6$	0001101
$x^4 v(x) = x^4 + x^5 + x^7 \equiv 1 + x^4 + x^5 (mod 1 + x^7)$	1000110
$x^5 v(x) = x^5 + x^6 + x^8 \equiv x + x^5 + x^6 (mod 1 + x^7)$	0100011
$x^6 v(x) = x^6 + x^7 + x^9 \equiv 1 + x^2 + x^6 (mod 1 + x^7)$	1010001

▲

تمهيدية (٤,٢,١٢)

لتكن C شفرة دورية ولتكن $v \epsilon C$، ولتكن $c(x) \epsilon \langle \{v(x), xv(x), \cdots, x^{n-1} v(x)\} \rangle$. عندئذ، توجد كثيرة حدود $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ بحيث يكون: $c(x) \equiv a(x) v(x) (mod 1 + x^n)$.

البرهان

بما أن $c(x) \epsilon \langle \{v(x), xv(x), \cdots, x^{n-1} v(x)\} \rangle$ فيوجد $a_0, a_1, \cdots, a_{n-1} \epsilon K$ بحيث يكون:

$$c(x) \equiv \left(a_0 v(x) + a_1 x v(x) + \cdots + a_{n-1} x^{n-1} v(x)\right) (mod 1 + x^n)$$

$$\equiv (a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) v(x) (mod 1 + x^n)$$

$$\equiv a(x) v(x) (mod 1 + x^n)$$

وهذا ينهي البرهان. ■

لتكن C شفرة خطية دورية. من الواضح أن C تحتوي كلمة غير صفرية g بحيث تكون درجة $g(x)$ أصغر ما يمكن ولتكن k. سنبرهن الآن أن g وحيدة. لنفرض أن $g'\epsilon C$ غير صفرية حيث $g'(x)$ درجتها k أيضاً. عندئذ، $g(x)+g'(x)=c(x)\epsilon C$ ؛ وذلك لأن C خطية. وبما أن $x^k+x^k=0$ فإن $deg\, c(x)<k$. وبهذا تكون $c(x)=0$ ونخلص إلى أن $g(x)=g'(x)$.

سنبرهن الآن أن كثيرة الحدود غير الصفرية التي درجتها أصغر ما يمكن تولّد الشفرة الخطية الدورية. ولهذا الغرض نفرض أن $c(x)\epsilon C$. بما أن $deg(c(x))\geq deg(g(x))$ فنجد استناداً إلى خوارزمية القسمة أن :

$c(x)=q(x)g(x)+r(x)$ أو $r(x)=q(x)g(x)+c(x)$.

ولكن استناداً إلى التمهيدية (**٤,٢,١٢**) نرى أن كلاً من $c(x)$ و $q(x)g(x)$ كلمة شفرة وبهذا تكون $r(x)$ كلمة شفرة. وبما أن $deg(g(x))\geq deg(r(x))$ فنرى أن $r(x)=0$. ومن ثم يكون $c(x)=q(x)g(x)$ وبهذا نرى أن $g(x)$ تولّد الشفرة C.

سنسمي كثيرة الحدود غير الصفرية ذات الدرجة الصغرى والتي تولّد الشفرة الخطية الدورية C، **كثيرة الحدود المولّدة (Generator Polynomial)** للشفرة C.

مبرهنة (٤,٢,١٣)

لتكن C شفرة دورية طولها n ولتكن $g(x)$ كثيرة الحدود المولّدة للشفرة C. إذا كان $deg(g(x))=n-k$ فإن :

(١) بُعد C يساوي k.

(٢) كلمات الشفرة المقابلة لكثيرات الحدود $g(x),xg(x),\cdots,x^{k-1}g(x)$ أساس للشفرة C.

(٣) $c(x)\epsilon C$ إذا وفقط إذا كان $c(x)=a(x)g(x)$ حيث $a(x)$ كثيرة حدود تُحقق $deg(a(x))<k$ (أي أن $g(x)$ قاسم لجميع كلمات الشفرة $c(x)$).

البرهان

إثبات الفقرة (٣) نحصل عليه من النقاش السابق للمبرهنة (**٤,٢,١٣**).

ولبرهان الفقرتين (١) و (٢) نفرض أن $deg(g(x)) = n - k$. عندئذ، $g(x), xg(x), \cdots, x^{k-1}g(x)$ مُستقلة خطياً (لماذا ؟). وبما أن $g(x)$ تقسم جميع كلمات الشفرة فنجد كثيرة حدود وحيدة $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ تُحقق :

$$c(x) = a(x)g(x) = a_0g(x) + a_1xg(x) + \cdots + a_{k-1}x^{k-1}g(x).$$

وبهذا يكون $c(x)\epsilon\langle\{g(x), xg(x), \cdots, x^{k-1}g(x)\}\rangle$. ونخلص إلى أن :

$\{g(x), xg(x), \cdots, x^{k-1}g(x)\}$ أساس للشفرة C. ■

مثال (٤,٢,١٤)

لنفرض أن $n = 7$ وأن $g(x) = 1 + x + x^3$ مولّد للشفرة الدورية C. أحد أساسات C هو :

$$g(x) = 1 + x + x^3 \leftrightarrow 1101000$$
$$xg(x) = x + x^2 + x^4 \leftrightarrow 0110100$$
$$x^2g(x) = x^2 + x^3 + x^5 \leftrightarrow 0011010$$
$$x^3g(x) = x^3 + x^4 + x^6 \leftrightarrow 0001101$$

لاحظ أن $x^4g(x)(mod1 + x^7) \equiv 1 + x^4 + x^5$ هي كلمة شفرة ؛ لأن :

$1 + x^4 + x^5 = (1 + x + x^2)(1 + x + x^3) = (1 + x + x^2)g(x).$ ▲

مثال (٤,٢,١٥)

لتكن C الشفرة الدورية $C = \{0000, 1010, 0101, 1111\}$. مجموعة كثيرات الحدود المقابلة هي $\{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\}$. لاحظ أن $1 + x^2 \leftrightarrow 1010$ هي كثيرة الحدود المولّدة للشفرة C ؛ وذلك لأن C تحتوي على كثيرة حدود واحدة فقط

من الدرجة الثانية ولا تحتوي كثيرات حدود من الدرجة الأولى. أيضاً كل من كلمات الشفرة (كثيرات الحدود) هي مضاعف لكثيرة الحدود المولّدة:

$$0 = 0(1 + x^2)$$
$$x + x^3 = x(1 + x^2)$$
$$1 + x^2 = 1(1 + x^2)$$
$$1 + x + x^2 + x^3 = (1 + x)(1 + x^2).$$ ▲

مثال (٤,٢,١٦)

من السهل التحقق من أن الشفرة:

$C = \{000000, 100100, 010010, 001001, 110110, 101101, 011011, 111111$

هي أصغر شفرة خطية طولها 6 وتحتوي على $100100 \leftrightarrow g(x) = 1 + x^3$. كثيرة الحدود الأصغرية التي تقابل كلمة شفرة هي $g(x) = 1 + x^3$ ولا تحتوي C على كثيرات حدود أخرى من الدرجة 3. وبهذا نرى أن $g(x) = 1 + x^3$ تولّد الشفرة C. الجدول (٤,٢) يُبيّن كلمات C كمضاعفات لكثيرة الحدود $g(x)$:

الجدول (٤,٢). كلمات الشفرة كمضاعفات لكثيرة الحدود المولّدة.

$f(x) = h(x)g(x)$	كثيرة الحدود $f(x)$	الكلمة
$0(1 + x^3)$	0	000000
$1(1 + x^3)$	$1 + x^3$	100100
$x(1 + x^3)$	$x + x^4$	010010
$x^2(1 + x^3)$	$x^2 + x^5$	001001
$(1 + x)(1 + x^3)$	$1 + x + x^3 + x^4$	110110
$(1 + x^2)(1 + x^3)$	$1 + x^2 + x^3 + x^5$	101101
$(x + x^2)(1 + x^3)$	$x + x^2 + x^4 + x^5$	011011
$(1 + x + x^2)(1 + x^3)$	$1 + x + x^2 + x^3 + x^4 + x^5$	111111

▲

من السهل توليد شفرة دورية وذلك باختيار كلمة v وحساب:

$$C = \langle\{v(x), xv(x), \cdots, x^{n-1}v(x)\}\rangle(mod 1 + x^n).$$

ولكننا بحاجة إلى إيجاد مولّد لهذه الشفرة وكتابة جميع كلمات C وهذه ليست الطريقة الملائمة لذلك. ولكن كثيرة الحدود المولّدة للشفرة الدورية تتمتع بالخاصية المهمة التالية:

مبرهنة (٤,٢,١٧)

$g(x)$ كثيرة حدود مولّدة للشفرة الخطية الدورية من الطول n إذا وفقط إذا كانت $g(x)$ تقسم $1+x^n$. أي أن $1+x^n = h(x)g(x)$.

البرهان

استناداً إلى التمهيدية (**٤,٢,١٢**) نجد أن:

$$c(x) = h(x)g(x)(mod1 + x^n) = h(x)g(x) + q(x)(1 + x^n)$$

كلمة شفرة لكل $h(x)$. واستناداً إلى خوارزمية القسمة نرى أن $g(x)$ تقسم أي كلمة شفرة $c(x)$ إذا وفقط إذا كانت $g(x)$ تقسم $1+x^n$. وبهذا نجد استناداً إلى المبرهنة (**٤,٢,١٣**) أن $g(x)$ تولّد الشفرة الدورية من الطول n إذا وفقط إذا كانت $g(x)$ تقسم $1+x^n$. ■

نتيجة (٤,٢,١٨)

لتكن $g(x)$ كثيرة الحدود المولّدة لأصغر شفرة دورية من الطول n تحتوي على الكلمة v (كثيرة الحدود $v(x)$). عندئذ، $g(x) = gcd(v(x), 1 + x^n)$.

البرهان

بما أن $g(x)$ كثيرة الحدود المولّدة للشفرة فنرى أن $g(x)$ تقسم كلاً من $v(x)$ و $1+x^n$. وبما أن $g(x)\epsilon\langle\{v(x), xv(x), \cdots, x^{n-1}v(x)\}\rangle$ فنجد أن $g(x) \equiv a(x)v(x)(mod1 + x^n)$. أي أن:

$$g(x) = a(x)v(x) + b(x)(1 + x^n).$$

الآن، إذا كانت $h(x)$ تقسم $v(x)$ و $1 + x^n$ فنرى أن $h(x)$ تقسم $a(x)v(x) + b(x)(1 + x^n)$. ومن ثم نجد أن $h(x)$ تقسم $g(x)$. إذن، $g(x) = gcd(v(x), 1 + x^n)$. ■

مثال (٤,٢,١٩)

لنفرض أن $n = 8$ وأن $v = 11011000$. أي أن $v(x) = 1 + x + x^3 + x^4$. بما أن:

$$gcd(v(x), 1 + x^8) = 1 + x^2$$

فنجد أن $g(x) = 1 + x^2$ كثيرة الحدود المولّدة لأصغر شفرة دورية تحتوي على $v(x)$ وبُعد هذه الشفرة يساوي $8 - 2 = 6$. ▲

من الممكن استخدام خوارزمية إقليدس لحساب القاسم المشترك الأعظم لكثيرتي حدود وهذه الطريقة موضّحة في الملحق A. من الممكن أيضاً استخدام العمليات الصفية الأولية لإيجاد كثيرة الحدود المولّدة لشفرة دورية طولها n وبُعدها $n - k$ ويتم ذلك على النحو التالي:

نقوم باختيار أساس (مصفوفة مولّدة) للشفرة ثم نستخدم العمليات الصفية الأولية للحصول على RREF حيث الأعمدة المتقدمة (عددها k) هي الأعمدة الأخيرة. عندئذ، يكون الصف (كلمة الشفرة) ذو الدرجة الصغرى هو كثيرة الحدود المولّدة.

تمارين

(**٤,٢,٢٠**) جد كثيرة الحدود المولّدة لأصغر شفرة خطية دورية تحتوي على الكلمة المبينة:

(أ) 010101 (ب) 010010

(ج) 01100110 (د) 0101100

(هـ) 001000101110000 (و) 000010010000000

(ز) 010111010000000.

(**٤,٢,٢١**) أعد التمرين (**٤,٢,٢٠**) لكل من الكلمات التالية:

(أ) 101010 (ب) 1100

(ج) 10001000 (د) 011011

(هـ) 10101 (و) 111111.

(**٤,٢,٢٢**) لكل من الشفرات $C = \langle S \rangle$ حيث S هي المجموعة المعطاة فيما يلي، جد كثيرة الحدود $g(x)$ المولّدة ومن ثم اكتب كلمات الشفرة كمضاعفات لكثيرة الحدود $g(x)$:

(أ) $S = \{010, 011, 111\}$.

(ب) $S = \{1010, 0101, 1111\}$.

(ج) $S = \{0101, 1010, 1100\}$.

(د) $S = \{1000, 0100, 0010, 0001\}$.

(هـ) $S = \{11000, 01111, 11110, 01010\}$.

(٤,٣) المصفوفات المولّدة ومصفوفات اختبار النوعية للشفرات الدورية

Generating & Parity Check Matrices for Cyclic Codes

يوجد عديد من المصفوفات المولّدة للشفرات الخطية الدورية، وأبسط هذه المصفوفات هي المصفوفة التي تتكون صفوفها من كلمات الشفرة المقابلة لكثيرة الحدود المولّدة وأول $k-1$ من ازاحاتها الدورية (انظر المبرهنة (**٤,٢,١٣**)):

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

مثال (٤,٣,١)

لتكن $C = \{0000,1010,0101,1111\}$ شفرة خطية دورية. كثيرة الحدود المولّدة للشفرة C هي $g(x) = 1 + x^2$. عندئذ، $n = 4$ و $k = 2$ ونرى أن أساساً للشفرة C هو:

$$g(x) = 1 + x^2 \leftrightarrow 1010$$

$$xg(x) = x + x^3 \leftrightarrow 0101$$

وبهذا تكون مصفوفة مولّدة للشفرة C هي $G = \begin{bmatrix} g(x) \\ xg(x) \end{bmatrix} = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}$. ▲

مثال (٤,٣,٢)

لتكن C شفرة خطية دورية من الطول $n = 7$ وكثيرة حدود مولّدة $g(x) = 1 + x + x^3$ من الدرجة $n - k = 3$. عندئذ، $k = 4$ وأساس للشفرة C هو:

$$g(x) = 1 + x + x^3$$

$$xg(x) = x + x^2 + x^4$$

$$x^2g(x) = x^2 + x^3 + x^5$$

$$x^3g(x) = x^3 + x^4 + x^6$$

ومصفوفة مولّدة للشفرة C هي:

$$G = \begin{bmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{bmatrix}.$$ ▲

لتكن C شفرة خطية دورية من الطول n والبُعد k (ومن ثم كثيرة الحدود المولّدة $g(x)$ من الدرجة $n - k$). عندئذ، إحداثيات المعلومات $(a_0, a_1, \cdots, a_{k-1})$ المراد تشفيرها (عددها k) تقابل كثيرة الحدود $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ وتُسمى **كثيرة حدود المعلومات أو كثيرة حدود الرسالة (Information or Message Polynomial)**.

عملية التشفير تتم بواسطة ضرب كثيرات حدود. أي أن $a(x)g(x) = c(x)$ هي عملية تشفير $a(x)$. وعليه نرى أنه يتم تخزين كثيرة الحدود المولّدة عوضاً عن تخزين المصفوفة المولّدة من الدرجة $k \times n$ وهذا تحسن ملحوظ عند حساب تعقد عملية التشفير.

إن العملية العكسية لضرب كثيرات الحدود هي قسمتها. ولهذا، نحصل على الرسالة المقابلة لأقرب كلمة شفرة $c(x)$ للكلمة المستقبلة بقسمة $c(x)$ على $g(x)$ ويكون خارج القسمة هو كثيرة حدود الرسالة $a(x)$.

مثال (٤,٣,٣)

لنفرض أن $g(x) = 1 + x + x^3$ و $n = 7$. عندئذ، $k = 7 - 3 = 4$. لنفرض أن $a(x) = 1 + x^2$ هي كثيرة حدود الرسالة والتي تقابل الكلمة $a = 1010$. يتم تشفير $a(x)$ على النحو التالي:

$$c(x) = a(x)g(x) = (1 + x^2)(1 + x + x^3) = 1 + x + x^2 + x^5$$

وبهذا تكون $c = 1110010$ هي كلمة الشفرة المقابلة. وإذا كانت $c(x) = 1 + x + x^4 + x^6$ فنجد أن كثيرة حدود الرسالة هي:

$$.a(x) = c(x)/g(x) = 1 + x^3$$

وتقابل الرسالة $a = 1001$. ▲

تمارين

(**٤,٣,٤**) لتكن $g(x) = 1 + x^2 + x^3$ كثيرة الحدود المولّدة للشفرة الخطية الدورية من الطول 7.

(أ) شفّر كثيرات حدود الرسائل التالية: $x + x^2 + x^3$ ، x ، $1 + x^3$.

(ب) جد كثيرة حدود الرسالة المقابلة لكل من كلمات الشفرة $c(x)$ التالية:

$$.x^4 + x^5 \text{ ، } 1 + x + x^2 + x^4 \text{ ، } x^2 + x^3 + x^4 + x^6$$

(**٤,٣,٥**) جد أساساً ومصفوفة مولّدة للشفرة الخطية الدورية من الطول n حيث كثيرة الحدود المولّدة المعطاة $g(x)$:

(أ) $.n = 7$ ، $g(x) = 1 + x^2 + x^3$

(ب) $.n = 9$ ، $g(x) = 1 + x^3 + x^6$

(ج) $g(x) = 1 + x + x^4$ ، $n = 15$.

(د) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ ، $n = 15$.

(هـ) $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$ ، $n = 15$.

(٤,٣,٦) أثبت أن الشفرة الخطية ذات المصفوفة المولّدة المعطاة G هي شفرة دورية وجد كثيرة حدودها المولّدة:

(أ) $G = \begin{bmatrix} 110110 \\ 001001 \\ 101101 \end{bmatrix}$ (ب) $G = \begin{bmatrix} 010101 \\ 111111 \end{bmatrix}$.

بعد أن وجدنا طريقة فعّالة للحصول على مصفوفة مولّدة للشفرة الخطية الدورية بدلالة كثيرة حدودها المولّدة، ننتقل إلى دراسة كيفية الحصول على مصفوفة اختبار النوعية لهذه الشفرات. ولهذا الغرض نحتاج إلى إيجاد مصفوفة H تحقق:

$wH = 0$ إذا وفقط إذا كانت w كلمة شفرة.

ولإنجاز ذلك نكتب بداية $w(x) = c(x) + e(x)$ حيث $c(x)$ هي كلمة شفرة و $e(x)$ كثيرة حدود الخطأ.

تُعرف **كثيرة حدود التناذر (Syndrome Polynomial)** $s(x)$ على أنها:

$$s(x) \equiv w(x)(mod\ g(x)).$$

إذا فرضنا أن درجة $g(x)$ تساوي $n-k$ فتكون درجة $s(x)$ أصغر من $n-k$ وتقابل كلمة ثنائية s من الطول $n-k$. وبما أن $w(x) = c(x) + e(x)$ و $c(x) = a(x)g(x)$ حيث $a(x)$ كثيرة حدود تنتمي إلى $K[x]$ فنرى أن $s(x) \equiv e(x)(mod\ g(x))$. أي أن كثيرة حدود التناذر تعتمد فقط على الخطأ.

لتكن H هي المصفوفة التي صفوفها الكلمات r_i من الطول $n-k$ المقابلة لكثيرات الحدود $r_i(x) \equiv x^i(mod\ g(x))$. عندئذ، H هي مصفوفة اختبار النوعية للشفرة. ولإثبات ذلك، نفرض أن w كلمة مستقبلة. عندئذ، $w(x) = c(x) + e(x)$ ويكون:

$$wH = (c+e)H = \sum_{i=0}^{n-1}(c_i+e_i)r_i$$
$$\Leftrightarrow \sum_{i=0}^{n-1}(c_i+e_i)\, r_i(x) \equiv (\sum_{i=0}^{n-1} c_i x^i)\, mod\ g(x) + (\sum_{i=0}^{n-1} e_i x^i)\, mod\ g(x)$$
$$\equiv c(x) mod\ g(x) + e(x) mod\ g(x)$$
$$\equiv 0 + e(x) mod\ g(x)$$
$$\equiv s(x)$$

وبهذا نجد أن $s(x) = 0$ إذا وفقط إذا كانت $w(x)$ كلمة شفرة. إذن، H مصفوفة اختبار النوعية. أيضاً، إذا كان $wH = s$ فنرى أن $s(x) \equiv w(x)(mod\ g(x))$. وبهذا يتضح السبب وراء تسمية $s(x)$ كثيرة حدود التناذر. سنستخدم هذا التمثيل للتناذر في الفصل السابع عند تصويب متتالية من الأخطاء.

مثال (٤,٣,٧)

لنفرض أن $n = 7$ وأن $g(x) = 1 + x + x^3$. عندئذ، $n - k = 3$ ونجد H كالتالي:

$$r_0(x) \equiv 1 mod\ g(x) = 1 \leftrightarrow 100$$
$$r_1(x) \equiv x mod\ g(x) = x \leftrightarrow 010$$
$$r_2(x) \equiv x^2 mod\ g(x) = x^2 \leftrightarrow 001$$
$$r_3(x) \equiv x^3 mod\ g(x) = 1 + x \leftrightarrow 110$$
$$r_4(x) \equiv x^4 mod\ g(x) = x + x^2 \leftrightarrow 011$$
$$r_5(x) \equiv x^5 mod\ g(x) = 1 + x + x^2 \leftrightarrow 111$$
$$r_6(x) \equiv x^6 mod\ g(x) = 1 + x^2 \leftrightarrow 101$$

وبهذا تكون $H = \begin{bmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 111 \\ 101 \end{bmatrix}$. إذا استقبلنا كثيرة الحدود $w(x) = 1 + x^5 + x^6$. أي الكلمة $w = 1000011$ فنرى أن $wH = s = 110$ وأن:

$s(x) = 1 + x \equiv 1 + x^5 + x^6 mod(1 + x + x^3) \equiv w(x)(mod\ g(x))$. ▲

تمارين

(**٤,٣,٨**) جد مصفوفة اختبار النوعية للشفرة الخطية الدورية من الطول 7 حيث كثيرة حدودها المولّدة هي $g(x) = 1 + x + x^2 + x^4$.

(**٤,٣,٩**) جد مصفوفة اختبار النوعية للشفرة الدورية من الطول n حيث كثيرة حدودها المولّدة هي $g(x)$:

(أ) $g(x) = 1 + x^2$ ، $n = 6$.

(ب) $g(x) = 1 + x^3$ ، $n = 6$.

(ج) $g(x) = 1 + x^2$ ، $n = 8$.

(د) $g(x) = 1 + x^3 + x^6$ ، $n = 9$.

(هـ) $g(x) = 1 + x + x^4$ ، $n = 15$ (هذه تولّد شفرة هامينغ).

(و) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ ، $n = 23$ (هذه تولّد شفرة جولاي).

(ز) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ ، $n = 15$ (هذه تولّد شفرة BCH التي تصوّب خطأين وسنناقشها في الفصل الخامس).

(٤,٤) إيجاد الشفرات الدورية

Finding Cyclic Codes

يلزمنا لإنشاء شفرة خطية دورية من الطول n والبُعد k إيجاد قاسم لكثيرة الحدود $1 + x^n$ من الدرجة $n - k$. في بعض الأحيان يوجد أكثر من قاسم واحد وفي أحيان أخرى لا يوجد مثل هذا القاسم. ومسألة مهمة أخرى هي مسألة إيجاد شفرة خطية مسافتها صغرى وهذه مسألة لا يوجد لها حل عام حتى الآن وسنؤجل نقاشها إلى وقت لاحق.

بما أن أي مولّد للشفرة الدورية من الطول n يقسم كثيرة الحدود $1 + x^n$ فلإيجاد جميع هذه الشفرات يتعيّن علينا إيجاد جميع قواسم $1 + x^n$ ويمكن إنجاز ذلك بإيجاد جميع القواسم **غير القابلة للتحليل (Irreducible)**.

نقول إن كثيرة الحدود $f(x)\epsilon K[x]$ التي درجتها أكبر من أو تساوي 1، **غير قابلة للتحليل (Irreducible)** إذا لم نستطع كتابتها كحاصل ضرب كثيرتي حدود في $K[x]$ درجة كل منهما على الأقل 1. إنه ليس بالأمر اليسير إيجاد القواسم غير القابلة للتحليل (ومن ثم جميع القواسم) لكثيرة الحدود $1 + x^n$. يُزوّدنا الملحق B بتحليل $1 + x^n$ لكل $n \leq 31$ إلى عوامل غير قابلة للتحليل، كما نقدم في المثال (**٤,٤,١٤**) طريقة لتحليل $1 + x^n$.

الشفرة الخطية الدورية المولّدة بالقاسم 1 لكثيرة الحدود $1 + x^n$ هي الشفرة التي بُعدها n (لأن درجة 1 تساوي 0) ومن ثم فهي الشفرة K^n. أيضاً الشفرة $C = \{0\}$ حيث 0 الكلمة الصفرية من الطول n هي شفرة دورية مولّدة بكثيرة الحدود $g(x) = 0 \equiv 1 + x^n (mod 1 + x^n)$. تُسمى كل من K^n و $\{0\}$ **شفرة دورية غير فعلية (Improper Cyclic Code)** وتُسمى جميع الشفرات الدورية الأخرى، **شفرات دورية فعلية (Proper Cyclic Codes)**.

مثال (٤,٤,١)

إذا كان $n = 3$ فنرى أن:

$$1 + x^3 = (1 + x)(1 + x + x^2)$$

هو تحليل $1 + x^3$ إلى عوامل غير قابلة للتحليل. وعليه توجد شفرتان فعليتان دوريتان من الطول 3. الأولى منهما مولّدة بكثيرة الحدود $g(x) = 1 + x$ ولها مصفوفة مولّدة $G = \begin{bmatrix} 110 \\ 011 \end{bmatrix}$، وهذه الشفرة هي $C = \{000, 110, 011, 101\}$. أما الشفرة الأخرى فهي مولّدة بكثيرة الحدود $g(x) = 1 + x + x^2$ ومصفوفتها المولّدة هي $G = [111]$. وبهذا تكون $C = \{000,111\}$. ▲

مثال (٤,٤,٢)

إذا كان $n = 6$ فإن تحليل $1 + x^6$ إلى عوامل غير قابلة للتحليل هو:

$$1 + x^6 = (1 + x^3)^2 = (1 + x)^2(1 + x + x^2)^2.$$

وعليه، لإيجاد مولّدات الشفرات الخطية الدورية الفعلية من الطول 6، نقوم بإيجاد جميع حواصل الضرب الممكنة لهذه العوامل (عدا 1 و $1 + x^6$). كل من حواصل الضرب هذه تولّد شفرة خطية دورية فعلية من الطول 6. الجدول التالي يُبيّن كلاً من هذه المولّدات وبُعد الشفرة التي يُولّدها.

البُعد	المولّد
5	$1 + x$
4	$(1 + x)^2 = 1 + x^2$
4	$1 + x + x^2$
2	$(1 + x + x^2)^2 = 1 + x^2 + x^4$
3	$(1 + x)(1 + x + x^2) = 1 + x^3$
2	$(1 + x)^2(1 + x + x^2) = 1 + x + x^3 + x^4$
1	$(1 + x)(1 + x + x^2)^2 = 1 + x + x^2 + x^3 + x^4 + x^5$. ▲

مبرهنة (٤,٤,٣)

إذا كان $n = 2^r s$ فإن $1 + x^n = (1 + x^s)^{2^r}$.

البرهان

باستخدام الاستقراء الرياضي على r. إذا كان $r = 1$ فإن $n = 2s$ ونرى أن:

$$(1 + x^s)^2 = 1 + x^s + x^s + x^{2s} = 1 + x^{2s}$$

وعليه فالعبارة صائبة عندما $r = 1$. لنفرض الآن أن العبارة صحيحة عند $r - 1$[٤].

حينئذ،

$$(1 + x^s)^{2^r} = \left[(1 + x^s)^{2^{r-1}}\right]^2$$

---

(٤) المترجمان: قمنا بكتابة تفاصيل خطوة الاستقراء للمبرهنة (٤,٤,٣).

$$= (1 + x^{2^{r-1}s})^2 \quad \text{(خطوة الاستقراء)}$$
$$= 1 + 2x^{2^{r-1}s} + x^{2^r s}$$
$$= 1 + x^{2^r s}$$

وبهذا تكون العبارة صحيحة عند r. ■

نتيجة (٤,٤,٤)

لنفرض أن $n = 2^r \cdot s$ حيث s عدد فردي ولنفرض أن $1 + x^s$ هي حاصل ضرب عدد z من كثيرات الحدود غير القابلة للتحليل. عندئذ، يوجد عدد $(2^r + 1)^z$ شفرة خطية دورية من الطول n ومن ثم يوجد عدد $(2^r + 1)^z - 2$ شفرة خطية دورية فعلية من الطول n. ■

مثال (٤,٤,٥)

بيّنا في المثال (٤,٤,١) أن $1 + x^3 = (1 + x)(1 + x + x^2)$ حيث كل من $1 + x$ و $1 + x + x^2$ غير قابلة للتحليل. باستخدام النتيجة (٤,٤,٤) حيث $r = 0$، $s = 3$، $z = 2$ نجد أن عدد الشفرات الخطية الدورية من الطول 3 هو $(2^0 + 1)^2 = 4$، منها شفرتان فعليتان كما هو مبيّن في المثال (٤,٤,١). أما لكثيرة الحدود $1 + x^6$ فلدينا $n = 6 = 2^1 \times 3$. عندئذ، $r = 1$، و $z = 2$ ويكون عدد الشفرات الخطية الدورية من الطول 6 هو $(2 + 1)^2 = 9$ حيث 7 منها فعلية وهذا ما وجدناه في المثال (٤,٤,١). ▲

تمارين

(٤,٤,٦) جد عدد الشفرات الخطية الدورية الفعلية من الطول n حيث:

(أ) $n = 4$ (ب) $n = 5$

(ج) $n = 7$ (د) $n = 14$

(هـ) $n = 56$ (و) $n = 15$

(ز) $n = 120$ (ح) $n = 1024$.

(**٤,٤,٧**) جد كثيرة الحدود المولّدة لجميع الشفرات الخطية الدورية من الطول n حيث :

(أ) $n = 4$ (ب) $n = 5$.

(**٤,٤,٨**) جد مولّدين من الدرجة 4 للشفرة الخطية الدورية من الطول 7.

(**٤,٤,٩**) جد مولّداً ومصفوفة مولّدة للشفرة الخطية الدورية من الطول n والبُعد k حيث :

(أ) $n = 12$ ، $k = 5$ (ب) $n = 12$ ، $k = 7$

(ج) $n = 14$ ، $k = 5$ (د) $n = 14$ ، $k = 6$

(هـ) $n = 14$ ، $k = 8$.

(**٤,٤,١٠**) أثبت أن شفرة جولاي C_{23} تكافئ شفرة خطية دورية.

نقدم الآن طريقة سهلة لإيجاد جميع الشفرات الدورية (أي عوامل $(1 + x^n)$) حيث n عدد فردي.

الخطوة الأولى من هذه الطريقة هي توليد جميع كثيرات الحدود $I(x)(mod 1 + x^n)$ التي تحقق $I(x) \equiv I(x)^2 (mod 1 + x^n)$. تُسمى كثيرات الحدود هذه **بكثيرات الحدود متساوية القوى (Idempotent Polynomials)**. إذا كانت كل من $u(x)$ و $v(x)$ كثيرة حدود متساوية القوى فمن السهل أن نرى أن كلاً من $u(x) + v(x)$ و $u(x)v(x)(mod\ 1 + x^n)$ كثيرة حدود متساوية القوى. نحتاج الآن لإنشاء مجموعة "أساسية" من كثيرات الحدود المتساوية القوى. ولهذا الغرض نجزئ المجموعة $\mathbb{Z}_n = \{0,1,2,\cdots,n-1\}$ إلى فصول تكافؤ. لنفرض أن :

$C_i = \{s \equiv 2^i \times i (mod\ n) : j = 0,1,\cdots,r\}$ حيث $1 \equiv 2^r (mod\ n)$.

مثال (٤,٤,١١)

إذا كان $n = 7$ فلدينا $C_3 = \{3,5,6\} = C_5 = C_7$ ، $C_1 = \{1,2,4\} = C_2 = C_4$ ، $C_0 = \{0\}$.

وإذا كان $n = 9$ فلدينا $C_3 = \{3,6\}$ ، $C_1 = \{1,2,4,8,7,5\}$ ، $C_0 = \{0\}$.

الآن، لكل فصل من فصول التكافؤ المختلفة C_i نجد كثيرة حدود مقابلة $c_i(x)$ حيث:

$$c_i(x) = \sum_{j \epsilon C_i} x^j$$

الآن، $c_i(x)$ كثيرة حدود متساوية القوى لأن:

$$c_i(x)^2 = c_i(x^2) = \sum_{j \epsilon C_i} x^{2j} \equiv \sum_{k \epsilon C_i} x^k \;(mod(1 + x^n))$$

وذلك لأنه إذا كان $j \epsilon C_i$ فإن $2j (mod\, n) \epsilon C_i$. لاحظ أيضاً، أنه إذا كانت $I(x)(mod(1 + x^n))$ كثيرة حدود متساوية القوى فإن:

$$I(x) = \sum_{i=0}^{k} a_i c_i(x) \quad \text{حيث} \quad a_i \epsilon \{0,1\}.$$ ▲

مثال (٤,٤,١٢)

إذا كان $n = 7$ فلدينا:

$C_0 = \{0\}$ ، $c_0(x) = x^0 = 1$

$C_1 = \{1,2,4\}$ ، $c_1(x) = x + x^2 + x^4$

$C_3 = \{3,5,7\}$ ، $c_3(x) = x^3 + x^6 + x^5$.

وبهذا، إذا كانت $I(x)(mod 1 + x^7)$ كثيرة حدود متساوية القوى فنرى أن:

$$I(x) = a_0 c_0(x) + a_1 c_1(x) + a_3 c_3(x)$$

حيث $a_i \epsilon \{0,1\}$. إذن، يوجد $2^3 - 1$ من كثيرات الحدود المتساوية القوى المختلفة قياس $1 + x^7$ (حيث تجاهلنا كثيرة الحدود المتساوية القوى التافهة $I(x) = 0$). ▲

المبرهنة التالية تقدم لنا العلاقة بين كثيرات الحدود المتساوية القوى والشفرات الدورية:

مبرهنة (٤,٤,١٣)

تحتوي أي شفرة دورية على كثيرة حدود متساوية القوى وحيدة وتولّد الشفرة.

البرهان

لتكن $g(x)$ كثيرة حدود مولّدة للشفرة الدورية من الطول n ولنفرض أن $g(x)h(x) = 1 + x^n$ حيث n فردي.حينئذ، $gcd(h(x), g(x)) = 1$. ونرى استناداً إلى خوارزمية إقليدس (ملحق A) وجود كثيرتي حدود $t(x)$ و $s(x)$ تحققان:

$$1 = t(x)g(x) + s(x)h(x)$$

وبهذا نجد أن:

$$\begin{aligned} t(x)g(x) &= (t(x)g(x))^2 + t(x)s(x)h(x)g(x) \\ &= (t(x)g(x))^2 + t(x)s(x)(1 + x^n) \\ &\equiv \left(t(x)g(x)\right)^2 (mod 1 + x^n) \end{aligned}$$

إذن، $t(x)g(x)$ كثيرة حدود متساوية القوى و $g(x) = \gcd(t(x)g(x), 1 + x^n)$. ■

مثال (٤,٤,١٤)

لإيجاد جميع الشفرات الدورية من الطول 9، يكفي أن نجد جميع كثيرات الحدود المتساوية القوى ومن ثم إيجاد كثيرات الحدود المولّدة المقابلة لها. بما أن:

$$C_0 = \{0\} \text{ ، } C_1 = \{1,2,4,8,7,5\} \text{ ، } C_3 = \{3,6\}$$

فنرى أن $c_0(x) = 1$ ، $c_1(x) = x + x^2 + x^4 + x^5 + x^7 + x^8$ ، $c_3(x) = x^3 + x^6$

وأن:

$$I(x) = a_0 c_0(x) + a_1 c_1(x) + a_3 c_3(x).$$

والجدول التالي يُبيّن $I(x)$ وكثيرة الحدود المولّدة المقابلة لها :

كثيرة الحدود المتساوية القوى $I(x)$	كثيرة الحدود المولّدة $g(x) \equiv gcd(I(x), 1 + x^9)$
1	1
$x + x^2 + x^4 + x^5 + x^7 + x^8$	$1 + x + x^3 + x^4 + x^6 + x^7$
$x^3 + x^6$	$1 + x^3$
$1 + x + x^2 + x^4 + x^5 + x^7 + x^8$	$1 + x + x^2$
$1 + x^3 + x^6$	$1 + x^3 + x^6$
$x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$	$1 + x$
▲ $.1 + x + x^2 + x^3 + x^5 + x^6 + x^7 + x^8$	$1 + x + x^2 + x^3 + x^5 + x^6 + x^7 + x^8$

تمرين

(٤,٤,١٥) جد جميع كثيرات الحدود المتساوية القوى قياس $1 + x^n$ وكثيرات الحدود المولّدة المقابلة لها لقيم n التالية :

(أ) $n = 5$ (ب) $n = 7$ (ج) $n = 11$

(د) $n = 15$ (هـ) $n = 31$.

(٤,٥) الشفرات الدورية الثنوية

Dual Cyclic Codes

إحدى الخواص المهمة للشفرات الدورية هي أن الشفرة الثنوية هي شفرة دورية أيضاً وسنقدم طريقة لإنشاء كثيرة حدود مولّدة للشفرة الثنوية.

سنبرهن الآن أن الشفرة الثنوية للشفرة الدورية هي دورية أيضاً. يعتمد هذا البرهان على الملاحظة التالية : إذا كان $a \cdot b = 0$ وكانت π الإزاحة الدورية فإن :

$$a \cdot b = a_0 b_0 + a_1 b_1 + \cdots + a_n b_n = 0$$
$$\Rightarrow \pi(a) \cdot \pi(b) = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n + a_0 b_0 = 0$$

لنفرض الآن أن C شفرة دورية مولّدة بالكلمة v. عندئذ،

$$C = \langle\{v, \pi(v), \cdots, \pi^{n-1}(v)\}\rangle.$$

إذا كانت $u \epsilon C^{\perp}$ فنجد أن $\pi^{i}(v) \cdot u = 0$ لكل $i = 0,1, \cdots, n-1$. وعليه فإن $\pi^{i+1}(v) \cdot \pi(u) = 0$ ويكون $\pi(u)$ متعامداً على $C = \langle\{\pi(v), \pi^{2}(v), \cdots, \pi^{n}(v)\}\rangle$؛ وذلك لأن $\pi^{n}(v) = v$. وبما أن $u \epsilon C^{\perp}$ يؤدي إلى أن $\pi(u) \epsilon C^{\perp}$ فنخلص إلى أن $C^{\perp}$ دورية.

لإيجاد مولِّد للشفرة الثنوية نحتاج إلى إيجاد علاقة بين ضرب كثيرات الحدود والضرب القياسي للمتجهات.

تمهيدية (٤,٥,١)

لنفرض أن $a \leftrightarrow a(x)$، $b \leftrightarrow b(x)$، $b' \leftrightarrow b'(x) \equiv x^{n} b(x^{-1})(mod 1 + x^{n})$. عندئذ، $a(x)b(x)(mod 1 + x^{n}) = 0$ إذا وفقط إذا كان $\pi^{k}(a) \cdot b' = 0$ لكل $k = 0,1, \cdots, n-1$.

البرهان

لنفرض أن $c(x) \equiv a(x)b(x)(mod 1 + x^{n})$. بملاحظة أن $x^{k} \equiv x^{n+k}(mod 1 + x^{n})$ فنجد أن معامل x^{k} في $c(x)$ هو:

$$c_{k} = a_{k}b_{0} + a_{k+1}b_{n-1} + \cdots + a_{n-1}b_{k+1} + a_{0}b_{k} + \cdots + a_{k-1}b.$$

الآن، إذا كان $a = (a_{0}, a_{1}, \cdots, a_{n-1})$ و $b = (b_{0}, b_{1}, \cdots, b_{n-1})$ فيكون:

$$b' = (b_{0}, b_{n-1}, b_{n-2}, \cdots, b_{1}) \text{ و } c_{k} = \pi^{k}(a) \cdot b'.$$

إذن، $c_{k} = 0$ لكل $k = 0,1, \cdots, n-1$. إذا وفقط إذا كان:

$$c(x) = 0 \equiv a(x)b(x)(mod 1 + x^{n}). \quad \blacksquare$$

لنفرض أن C شفرة خطية دورية من الطول n وأن $g(x)$ كثيرة حدود مولّدة للشفرة C. حينئذ، $g(x)$ تقسم $x^{n} + 1$ ومن ثم توجد كثيرة حدود وحيدة $h(x)$ تحقق $g(x)h(x) = 1 + x^{n}$. واستناداً إلى التمهيدية (**٤,٥,١**) نعلم أن $x^{n}h(x^{-1}) \epsilon C^{\perp}$.

مبرهنة (٤,٥,٢)

لنفرض أن C شفرة خطية دورية من الطول n والبُعد k ولنفرض أن $g(x)$ كثيرة حدود مولّدة للشفرة C. إذا كان $1 + x^n = g(x)h(x)$ فإن $C^\perp$ شفرة دورية من البُعد $n - k$ و $x^n h(x^{-1})$ كثيرة حدود مولّدة لها.

البرهان

بما أن بُعد C يساوي k ودرجة $g(x)$ تساوي $n - k$ فتكون درجة $h(x)$ تساوي k.
وبما أن $g(x)h(x) = 1 + x^n$ فنرى أن $g(x^{-1})h(x^{-1}) = 1 + (x^{-1})^n$ وأن:

$$x^n g(x^{-1})h(x^{-1}) = x^n(1 + x^{-n})$$

$$x^{n-k} g(x^{-1}) x^k h(x^{-1}) = 1 + x^n$$

إذن، $x^k h(x^{-1})$ قاسم لكثيرة الحدود $1 + x^n$ درجتها تساوي k وبهذا تكون مولّدة للشفرة الخطية الدورية $C^\perp$ ذات البُعد $n - k$ التي تحتوي $x^n h(x^{-1})$. ■

مثال (٤,٥,٣)

كثيرة الحدود $g(x) = 1 + x + x^3$ تولّد شفرة خطية دورية من الطول 7 والبُعد $k = 7 - 3 = 4$. وبما أن $g(x)$ قاسم لكثيرة الحدود $1 + x^7$ فنستطيع إيجاد كثيرة حدود $h(x)$ تحقق $1 + x^7 = g(x)h(x)$. ونرى بالقسمة المطوّلة أن $h(x) = 1 + x + x^2 + x^4$.
إذن، كثيرة الحدود المولّدة للشفرة $C^\perp$ هي:

$$g^\perp(x) = x^4 h(x^{-1}) = x^4(1 + x^{-1} + x^{-2} + x^{-4}) = 1 + x^2 + x^3 + x^4$$

وتقابل الكلمة $w = 1011100$. من الواضح أن $g \cdot w = (11010000)(1011100)$ وأن $\pi^k(g) \cdot w = 0$. لاحظ أن $g^\perp(x) \neq h(x)$ في هذا المثال. ▲

مثال (٤,٥,٤)

كثيرة الحدود $g(x) = 1 + x + x^2$ تولّد شفرة خطية دورية من الطول 6 وكثيرة الحدود $h(x)$ التي تحقق $g(x)h(x) = 1 + x^6$ هي $h(x) = 1 + x + x^3 + x^4$. إذن،

$g^{\perp}(x) = x^4 h(x^{-1}) = x^4(1 + x^{-1} + x^{-2} + x^{-4}) = x^4 + x^3 + x + 1$ هي كثيرة حدود مولّدة للشفرة الثنوية. لاحظ أن $g^{\perp}(x) = h(x)$ في هذا المثال. ▲

تمرين

(٤,٥,٥) جد كثيرة حدود مولّدة لشفرة ثنوية للشفرة الدورية من الطول n التي كثيرة حدودها المولّدة $g(x)$ هي:

(أ) $g(x) = 1 + x^2$ ، $n = 6$.

(ب) $g(x) = 1 + x^3$ ، $n = 6$.

(ج) $g(x) = 1 + x^2$ ، $n = 8$.

(د) $g(x) = 1 + x^3 + x^6$ ، $n = 9$.

(هـ) $g(x) = 1 + x + x^4$ ، $n = 15$.

(و) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ ، $n = 15$.

(ز) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ ، $n = 23$.

(ح) $g(x) = 1 + x + x^2 + x^4$ ، $n = 7$.

الفصل الخامس

شفرات BCH
BCH Codes

(٥,١) الحقول المنتهية
Finite Fields

نقدم في هذا الفصل صنفاً خاصاً من الشفرات الدورية ونوظّف حقول جالوا $GF(2^r)$ لإيجاد طريقة أخرى لفك تشفيرها.

تذكر أن كثيرة الحدود $d(x)$ تكون قاسماً أو عاملاً لكثيرة الحدود $f(x)$ إذا كان $f(x) = g(x)d(x)$. من الواضح أن 1 و $f(x)$ قاسمان (تافهان) لأي كثيرة حدود $f(x)$. يُسمى أي قاسم آخر **قاسماً غير تافه أو قاسماً فعلياً (Nontrivial or Proper Divisor)** لكثيرة الحدود $f(x)$.

نقول إن كثيرة الحدود $f(x)\epsilon K[x]$ **غير قابلة للتحليل على K (Irreducible Over K)** إذا لم يكن لها قواسم فعلية في $K[x]$. وإذا وجد لها قواسم فعلية فتكون **قابلة للتحليل على K (Reducible or Factorable Over K)**.

مثال (٥,١,١)

من الواضح أن كلاً من x و $x+1$ غير قابلة للتحليل (هذه هي كثيرات الحدود من الدرجة الأولى على K). كما أن x^2+x+1 غير قابلة للتحليل ؛ لأن x و $x+1$

لا تقسمانها. ولكن x قاسم لكثيرتي الحدود x^2 و $x + x^2$ وأن $1 + x$ قاسم لكثيرة الحدود $1 + x^2$. وبهذا نرى أن كثيرات الحدود x^2 ، $1 + x^2$ ، $x + x^2$ قابلة للتحليل. ▲

لاحظ أن $1 + x$ قاسم لكثيرة الحدود $f(x)$ إذا وفقط إذا كان $f(1) = 0$ وأن x قاسم لكثيرة الحدود $g(x)$ إذا وفقط إذا كان $g(0) = 0$. فمثلاً $1 + x$ قاسم لكثيرة الحدود $f(x) = 1 + x^2$ لأن $f(1) = 1 + 1 = 0$. نُلفت نظر القارئ إلى أن عملية إيجاد قواسم غير قابلة للتحليل لكثيرة حدود ليست بالأمر البسيط ونقصر بحثنا عن هذه القواسم في الوقت الحالي على التجريب.

مثال (٥,١,٢)

إذا كانت $f(x) = 1 + x + x^2 + x^3$ فنرى أن $f(1) = 1 + 1 + 1 + 1 = 0$ ومن ثم تكون $1 + x$ قاسماً لكثيرة الحدود $f(x)$. وبالقسمة المطوّلة نجد أن $f(x) = (1 + x)(1 + x^2) = (1 + x)^3$. أما إذا كانت $g(x) = 1 + x + x^3$ فنرى أن $g(0) = 1 \neq 0$ وأن $g(1) = 1 \neq 0$. وبهذا لا يوجد قواسم خطية لكثيرة الحدود $g(x)$. إذن، $g(x)$ غير قابلة للتحليل على K؛ لأنه لو كانت كثيرة الحدود من الدرجة الثالثة قابلة للتحليل لكان لها قاسم خطي. ▲

مثال (٥,١,٣)

إذا كانت $f(x) = 1 + x + x^4$ فنرى أن $f(0) \neq 0$ و $f(1) \neq 0$ ومن ثم ليس لها قاسم خطي. وعليه، إذا كانت $f(x)$ قابلة للتحليل فيجب أن يكون لها قاسم من الدرجة الثانية. ولكن كثيرة الحدود الوحيدة غير القابلة للتحليل من الدرجة الثانية على K هي $g(x) = 1 + x + x^2$. وبقسمة $f(x)$ على $g(x)$ نحصل على باق غير صفري. وبهذا نرى أن $1 + x + x^2$ ليس قاسماً لكثيرة الحدود $f(x)$. إذن، $f(x)$ غير قابلة للتحليل على K. ▲

تمارين

(٥,١,٤) بيّن ما إذا كانت كثيرة الحدود غير قابلة للتحليل على K:

(أ) $f(x) = 1 + x^2 + x^4$ (ب) $f(x) = 1 + x^8$

(ج) $f(x) = 1 + x^2 + x^3 + x^5$ (د) $f(x) = 1 + x^2 + x^6$

(هـ) $f(x) = 1 + x^4 + x^5$ (و) $f(x) = 1 + x + x^3 + x^7$.

(٥,١,٥) جد جميع كثيرات الحدود غير القابلة للتحليل على K من الدرجة 3 والدرجة 4.

(٥,١,٦) جد جميع كثيرات الحدود غير القابلة للتحليل على K من الدرجة 5.

نقول إن كثيرة الحدود غير القابلة للتحليل على K من الدرجة $n > 1$ هي **كثيرة حدود بدائية (Primitive Polynomial)** إذا لم تكن قاسماً لكثيرة الحدود $1 + x^m$ لكل $m < 2^n - 1$. سنبيّن أن أي كثيرة حدود غير قابلة للتحليل من الدرجة n يجب أن تكون قاسماً لكثيرة الحدود $1 + x^m$ عندما يكون $m = 2^n - 1$.

مثال (٥,١,٧)

كثيرة الحدود $1 + x + x^2$ غير قابلة للتحليل ولا تقسم $1 + x^m$ لكل $m < 3 = 2^2 - 1$ وبهذا فهي بدائية. كذلك، كثيرة الحدود $1 + x + x^3$ غير قابلة للتحليل وليست قاسماً لكثيرة الحدود $1 + x^m$ لكل $m < 7 = 2^3 - 1$ وبهذا فهي بدائية. أما كثيرة الحدود $f(x) = 1 + x + x^2 + x^3 + x^4$ فهي غير قابلة للتحليل (انظر التمرين (٥,١,٥)) ولكن:

$$1 + x^5 = (1 + x)(1 + x + x^2 + x^3 + x^4)$$

و $5 < 15 = 2^4 - 1$. إذن، $f(x) = 1 + x + x^2 + x^3 + x^4$ ليست بدائية. ▲

تذكر أن بإمكاننا تعريف الجمع والضرب لكثيرات الحدود قياس كثيرة حدود $h(x)$ من الدرجة n. لنفرض أن $K^n[x]$ هي مجموعة جميع كثيرات حدود $K[x]$ التي درجاتها أصغر من n. وبما أن كل كلمة من كلمات K^n تقابل كثيرة حدود تنتمي إلى $K^n[x]$ فبالإمكان تعريف الجمع والضرب لكلمات K^n.

نقدم في هذا الفصل بعض خصائص الحقول المنتهية التي تساعدنا على إنشاء وفك تشفير بعض الشفرات. لقد سبق وعرفنا عمليتي الجمع والضرب على K^n ولكن لكي يكون هذا النظام حقلاً يجب توخي الحذر عند اختيارنا لكثيرة الحدود $h(x)$. فمثلاً، في الحقل يجب أن تتحقق خاصية الاختصار التالية: إذا كان $ab = 0$ فإن $a = 0$ أو $b = 0$.

مثال (٥,١,٨)

إذا استخدمنا عملية ضرب كثيرات الحدود قياس $1 + x^4$ لتعريف عملية ضرب كلمات K^4 فحينئذ، نرى أن:

$$\begin{aligned}(0101)(0101) &\leftrightarrow (x + x^3)(x + x^3)\\ &= x^2 + x^6\\ &\equiv (x^2 + x^2)(mod 1 + x^4)\\ &= 0\\ &\leftrightarrow 0000\end{aligned}$$

وبهذا يكون $(0101)(0101) = 0000$. ولكن $0101 \neq 0000$ في K^4. إذن، K^4 ليس حقلاً بهذا الاختيار لكثيرة الحدود. ▲

تكمن المشكلة الأساسية في المثال السابق في أن $1 + x^4$ قابلة للتحليل على K. ولكي يكون K^n حقلاً تحت عملية الضرب المبيّنة، يجب أن تكون كثيرة حدود القياس كثيرة حدود من الدرجة n غير قابلة للتحليل. في هذه الحالة يكون هذا الحقل هو حقل جالوا $GF(2^n)$ ونترك اثبات ذلك لمقرر في الجبر المجرد.

مثال (٥,١,٩)

إذا استخدمنا كثيرة الحدود غير القابلة للتحليل $h(x) = 1 + x + x^4$ لتعريف عملية الضرب في K^4 فنجد أن:

$$\begin{aligned}(1101)(0101) &\leftrightarrow (1 + x + x^3)(x + x^3)\\ &= x + x^2 + x^3 + x^6\\ &\equiv x(mod 1 + x + x^4)\end{aligned}$$

وبهذا نرى أن $(1101)(0101) = 0100 \leftrightarrow x$. ▲

تمارين

(**٥,١,١٠**) باستخدام $h(x) = 1 + x + x^4$ لتعريف عملية الضرب في K^4. احسب حواصل الضرب التالية:

(أ) $(0011)(1011)$ (ب) $(1110)(1001)$

(ج) $(1010)(0110)$ (د) $(0100)(0010)$

(هـ) $(1110)(0111)$ (و) $(1111)(0001)$.

(**٥,١,١١**) جد حواصل ضرب جميع عناصر K^2 مُستخدماً $1 + x + x^2$ لتعريف عملية الضرب (أي أنشئ جدول الضرب).

مثال (٥,١,١٢)

في هـذا المثال، نقـوم بإنشاء $GF(2^3)$ باستـخدام كثيرة الحـدود البـدائيـة $h(x) = 1 + x + x^3$ لتعريف عملية الضرب. لإنجاز ذلك نحسب $x^i(mod\ h(x))$:

الكلمة	$\leftrightarrow$	$x^i(mod\ h(x))$
100		1
010		x
001		x^2
110		$x^3 \equiv 1 + x$
011		$x^4 \equiv x + x^2$
111		$x^5 \equiv 1 + x + x^2$
101		$x^6 \equiv 1 + x^2$

لحساب $(1 + x)x^2 \leftrightarrow (110)(001)$ لاحظ أولاً أن $1 + x \equiv x^3(mod\ h(x))$ (من الجدول المقدم سابقاً). وبهذا يكون:

$$\begin{aligned} x^2(1 + x) &\equiv x^2 \cdot x^3 \\ &\equiv x^5 \\ &\equiv 1 + x + x^2(mod\ h(x)) \end{aligned}$$

إذن، $(110)(001) = 111$. ▲

إن استخدام كثيرة حدود بدائية لإنشاء $GF(2^r)$ أفضل من استخدام كثيرة حدود غير قابلة للتحليل وليست بدائية ويرجع السبب في ذلك إلى سهولة إجراء العمليات الحسابية في حالة استخدام كثيرة الحدود البدائية، فإذا كانت $\beta \in K^n$ تقابل كثيرة الحدود $x(mod\ h(x))$ حيث $h(x)$ بدائية من الدرجة n فيكون $\beta^i \leftrightarrow x^i(mod\ h(x))$. وبملاحظة أن $1 \equiv x^m(mod\ h(x))$ نرى أن $h(x)$ تقسم $1 + x^m$ ولكن $h(x)$ لا تقسم $1 + x^m$ لكل $m < 2^n - 1$ لكونها بدائية. إذن، $\beta^m \neq 1$ لكل $m < 2^n - 1$. وبما أن $\beta^j = \beta^i$ حيث $j \neq i$ إذا وفقط إذا كان $\beta^i = \beta^{j-i}\beta^i$ فنرى أن $\beta^{j-i} = 1$. إذن،

$$K^n \backslash \{0\} = \{\beta^i : i = 0,1,\cdots,2^n - 2\}$$

وبهذا نستطيع كتابة الكلمات غير الصفرية في K^n كقوى للعنصر β وبهذا تكون عملية الضرب في الحقل سهلة جداً.

نقول إن العنصر $\alpha \in GF(2^r)$ **بدائي (Primitive)** إذا كان $\alpha^m \neq 1$ لكل $1 \leq m < 2^r - 1$. أي أن α عنصر بدائي إذا وفقط إذا كانت جميع كلمات $GF(2^r)$ غير الصفرية قوى للعنصر α.

من النقاش المُبيّن في الفقرة السابقة نجد أن الكلمة $\beta \leftrightarrow x(mod\ h(x))$ عنصر بدائي في الحقل $GF(2^r)$ المنشأ باستخدام كثيرة الحدود البدائية $h(x)$.

مثال (٥,١,١٣)

الجدول (**٥,١**) يُبيّن إنشاء الحقل $GF(2^4)$ باستخدام كثيرة الحدود البدائية $h(x) = 1 + x + x^4$ حيث العناصر ممثلة كقوى للعنصر $\beta \leftrightarrow x(mod\ h(x))$. لاحظ أن $\beta^{15} = 1$.

الجدول (٥,١). إنشاء $GF(2^4)$ باستخدام $h(x) = 1 + x + x^4$.

قوى β	كثيرة الحدود في x قياس $h(x)$	الكلمة
–	0	0000
$\beta^0 = 1$	1	1000
β	x	0100
β^2	x^2	0010
β^3	x^3	0001
β^4	$1 + x \equiv x^4$	1100
β^5	$x + x^2 \equiv x^5$	0110
β^6	$x^2 + x^3 \equiv x^6$	0011
β^7	$1 + x + x^3 \equiv x^7$	1101
β^8	$1 + x^2 \equiv x^8$	1010
β^9	$x + x^3 \equiv x^9$	0101
β^{10}	$1 + x + x^2 \equiv x^{10}$	1110
β^{11}	$x + x^2 + x^3 \equiv x^{11}$	0111
β^{12}	$1 + x + x^2 + x^3 \equiv x^{12}$	1111
β^{13}	$1 + x^2 + x^3 \equiv x^{13}$	1011
β^{14}	$1 + x^3 \equiv x^{14}$	1001

يتم حساب (1101)(0110) على النحو التالي:

$$(0110)(1101) = \beta^5 \cdot \beta^7 = \beta^{12} = 1111$$

لأن $(x + x^2)(1 + x + x^3) \equiv x^5 \cdot x^7 = x^{12} (mod\ h(x))$. ▲

تمارين

(٥,١,١٤) استخدم الجدول (٥,١) لحساب حواصل الضرب في K^4 للعناصر المقدمة في التمرين (٥,١,١٠).

(٥,١,١٥) أنشئ الحقول التالية بأسلوب المثال (٥,١,١٣):

(أ) $GF(2^2)$.

(ب) $GF(2^3)$ باستخدام $h(x) = 1 + x^2 + x^3$.

(ج) $GF(2^4)$ باستخدام $h(x) = 1 + x^3 + x^4$.

(د) $GF(2^5)$ باستخدام $h(x) = 1 + x^2 + x^5$.

(**٥,١,١٦**) إذا كانت $h(x) \epsilon K[x]$ كثيرة حدود غير قابلة للتحليل من الدرجة n فأثبت وجود $m \le 2^n - 1$ بحيث تقبل كثيرة الحدود $1 + x^m$ القسمة على $h(x)$.

(**٥,١,١٧**) جد جميع العناصر البدائية في الحقل $GF(2^4)$ (انظر الجدول (**٥,١**)).

(**٥,١,١٨**) أثبت أن $\beta^i \epsilon GF(2^r)$ عنصر بدائي إذا وفقط إذا كان $gcd(i, 2^r - 1) = 1$.

(٥,٢) كثيرات الحدود الأصغرية

Minimal Polynomials

نعلم أنه إذا كان $\epsilon\alpha F = GF(2^r)$ فإن α جذر لكثيرة الحدود $p(x)\epsilon F[x]$ إذا وفقط إذا كان $p(\alpha) = 0$. أي أنه إذا كانت $p(x) = a_0 + a_1 x + \cdots + a_k x^k = 0$ فإن $p(\alpha) = a_0 + a_1 \alpha + \cdots + a_k \alpha^k = 0$.

مثال (٥,٢,١)

لنفرض أن $p(x) = 1 + x^3 + x^4$ وأن β هو العنصر البدائي في الحقل $GF(2^4)$ المنشأ باستخدام كثيرة الحدود $h(x) = 1 + x + x^4$ (انظر الجدول (**٥,١**)). عندئذ،

$$\begin{aligned} p(\beta) = 1 + \beta^3 + \beta^4 &= 1000 + 0001 + 1100 \\ &= 0101 \\ &= \beta^9 \end{aligned}$$

ولذا فإن β ليس جذراً لكثيرة الحدود $p(x)$. ولكن:

$$\begin{aligned} p(\beta^7) &= 1 + (\beta^7)^3 + (\beta^7)^4 \\ &= 1 + \beta^{21} + \beta^{28} \\ &= 1 + \beta^6 + \beta^{13} && (\text{لأن } \beta^{15} = 1) \\ &= 1000 + 0011 + 1011 + 0000 = 0 \end{aligned}$$

وعليه يكون β^7 جذراً لكثيرة الحدود $p(x)$. لاحظ أننا استخدمنا $1 \leftrightarrow 1000$ و $0 \leftrightarrow 0000$ و $\beta^{15} = 1$. فمثلاً، لدينا $\beta^{21} = \beta^{15}\beta^6 = 1 \cdot \beta^6 = \beta^6$. أيضاً، $\beta^{28} = \beta^{15}\beta^{13} = 1 \cdot \beta^{13} = \beta^{13}$. ▲

ليكن $0 \neq \alpha\epsilon GF(2^r)$. تُعرف **رتبة العنصر α (Order of α)** غير الصفري على أنها أصغر عدد صحيح موجب m يحقق $\alpha^m = 1$. إذا كان m هو رتبة العنصر غير الصفري $\alpha\epsilon GF(2^r)$ فنرى أن $m \leq 2^r - 1$. وعلى وجه الخصوص يكون α عنصراً بدائياً إذا كان $m = 2^r - 1$.

تُعرف **كثيرة حدود $\alpha\epsilon GF(2^r)$ الأصغرية (Minimal Polynomial of α)** على أنها كثيرة الحدود في $K[x]$ ذات الدرجة الصغرى التي يكون α جذراً لها، ويُرمز لها بالرمز $m_\alpha(x)$. لاحظ أنه إذا كانت رتبة α تساوي m (أي، $\alpha^m = 1$) فإن α جذر لكثيرة الحدود $1 + x^m$. عليه، فكل عنصر من عناصر $GF(2^r)$ هو جذر لكثيرة حدود ما في $K[x]$.

تُساعدنا الحقائق التالية في إيجاد كثيرات الحدود الأصغرية لعناصر الحقل $GF(2^r)$.

مبرهنة (٥,٢,٢)

ليكن $\alpha \neq 0$ عنصراً في الحقل $GF(2^r)$ ولتكن $m_\alpha(x)$ كثيرة حدود α الأصغرية. عندئذ:

(أ) $m_\alpha(x)$ غير قابلة للتحليل على K.

(ب) إذا كانت $f(x)\epsilon K[x]$ حيث $f(\alpha) = 0$ فإن $m_\alpha(x)$ تقسم $f(x)$.

(ج) $m_\alpha(x)$ وحيدة.

(د) $m_\alpha(x)$ تقسم $1 + x^{2^r - 1}$.

البرهان

(أ) لنفرض أن $m_\alpha(x) = g(x)h(x)$. عندئذ، $m_\alpha(\alpha) = g(\alpha)h(\alpha) = 0$ ونرى أن $g(\alpha) = 0$ أو $h(\alpha) = 0$. بما أن $m_\alpha(x)$ أصغرية حيث $m_\alpha(\alpha) = 0$ فنجد أن $g(x) = 1$ أو $h(x) = 1$. وبهذا تكون $m_\alpha(x)$ غير قابلة للتحليل.

(ب) باستخدام خوارزمية القسمة نجد أن:

$$f(x) = m_\alpha(x)g(x) + r(x)$$

حيث $r(x) = 0$ أو $deg\, r(x) < deg\, m_\alpha(x)$. الآن

$$\begin{aligned} 0 = f(\alpha) &= m_\alpha(x)g(\alpha) + r(\alpha) \\ &= 0 \cdot g(\alpha) + r(\alpha) = r(\alpha) \end{aligned}$$

وباستخدام أصغرية درجة $m_\alpha(x)$ نرى أن $r(x) = 0$. وبهذا نرى أن $m_\alpha(x)$ تقسم $f(x)$.

(ج) لنفرض أن $m'(x)$ كثيرة حدود أصغرية أخرى للعنصر α. عندئذ، باستخدام الفقرة (ب) نرى أن $m'(x)$ تقسم $m_\alpha(x)$ وأن $m_\alpha(x)$ تقسم $m'(x)$. وبهذا يكون $m_\alpha(x) = m'(x)$. ونخلص إلى أن $m_\alpha(x)$ وحيدة.

(د) لنفرض أن β عنصر بدائي في الحقل $GF(2^r)$ وأن $\alpha = \beta^i$. عندئذ،

$$\alpha^{2^r-1} = (\beta^i)^{2^r-1} = (\beta^{2^r-1})^i = 1^i = 1$$

ونرى أن α جذر لكثيرة الحدود $1 + x^{2^r-1}$. واستناداً إلى الفقرة (ب) نجد أن $m_\alpha(x)$ قاسم لكثيرة الحدود $1 + x^{2^r-1}$. ■

لإيجاد كثيرة حدود α الأصغرية حيث $\alpha \epsilon GF(2^r)$ يكفي أن نجد تركيباً خطياً للمتجهات $\{1, \alpha, \alpha^2, \cdots, \alpha^r\}$ حيث $1 + \alpha + \alpha^2 + \cdots + \alpha^r = 0$. إن ضمان وجود مثل هذا التركيب الخطي يرجع إلى أن أي مجموعة جزئية من K^r عدد عناصرها $r + 1$ يجب أن تكون مرتبطة خطياً.

عند استخدام كثيرة حدود بدائية لإنشاء $GF(2^r)$ يكون من الطبيعي تمثيل $m_\alpha(x)$ بكثيرة الحدود $m_i(x)$ حيث $\alpha = \beta^i$. سنوضح ذلك في المثال التالي.

مثال (٥,٢,٣)

ليكن $\alpha = \beta^3 \epsilon GF(2^4)$ حيث استخدمنا $h(x) = 1 + x + x^4$ لإنشاء $GF(2^4)$ (انظر الجدول (**٥,١**)). كثيرة حدود α الأصغرية هي :

$$m_\alpha(x) = m_3(x) = a_0 + a_1 x + a_2 \alpha^2 + a_3 \alpha^3 + a_4 \alpha^4$$

ولإيجادها يتوجب علينا إيجاد القيم $a_0, a_1, \cdots, a_4 \epsilon\{0,1\}$. وبملاحظة أن :

$$\begin{aligned} m_\alpha(\alpha) = 0 &= a_0 1 + a_1 + a_2 + a_3 + a_4 \\ &= a_0\beta^0 + a_1\beta^3 + a_2\beta^6 + a_3\beta^9 + a_4\beta^{12} \end{aligned}$$

نرى أن :

$$0000 = a_0(1000) + a_1(0001) + a_2(0011) + a_3(0101) + a_4(1111).$$

وبحل هذا النظام لإيجاد a_0, a_1, a_2, a_3, a_4 نحصل على $a_0 = a_1 = a_2 = a_3 = a_4 = 1$.

وبهذا تكون $m_\alpha(x) = 1 + x + x^2 + x^3 + x^4$. جذور $m_\alpha(x)$ هي :

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\} = \{\beta^3, \beta^6, \beta^{12}, \beta^9\}.$$

وعليه يكون :

$m_3(x) = m_6(x) = m_9(x) = m_{12}(x)$ حيث $m_i(x)$ هي كثيرة حدود β^i الأصغرية. ▲

إذا أردنا إيجاد كثيرات الحدود الأصغرية لجميع عناصر $GF(2^4)$ فنحتاج إلى الحقائق المهمة التالية : تذكر أن $f(x)^2 = f(x^2)$. عندئذ ،

$$\left(\sum_{i=0}^{n} a_i x^i\right)^2 = \sum_{i=0}^{n} a_i^2 (x^i)^2 = \sum_{i=0}^{n} a_i (x^2)^i$$

حيث استخدمنا الحقيقة $(a+b)^2 = a^2 + b^2$ والحقيقة $a_i^2 = a_i$ ؛ لأن $a_i \epsilon \{0,1\}$.

عندئذ ، إذا كان $f(\alpha) = 0$ فنرى أن $f(\alpha^2) = (f(\alpha))^2 = 0$ ويكون α^2 جذراً آخر لكثيرة الحدود $f(x)$. وبالمثل $f(\alpha^4) = (f(\alpha^2))^2 = 0$ وهكذا. وبهذا نرى أنه إذا كان α

جذراً لكثيرة الحدود $f(x)$ فإن $\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^i}$ جذور لها أيضاً. وبقليل من الجهد يمكن إثبات :

مبرهنة (٥,٢,٤)

إذا كانت $m_\alpha(x)$ كثيرة حدود $\alpha \epsilon GF(2^r)$ الأصغرية فإن $\left\{\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{r-1}}\right\}$ هي جميع جذور $m_\alpha(x)$. وعلى وجه الخصوص درجة $m_\alpha(x)$ تساوي $\left|\left\{\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{r-1}}\right\}\right|$.

مثال (٥,٢,٥)

لنفرض أن $m_5(x)$ كثيرة حدود $\alpha = \beta^5$ حيث α عنصر في الحقل $GF(2^4)$ المنشأ في الجدول (**٥,١**). استناداً إلى المبرهنة (**٥,٢,٤**) نجد أن $\{\beta^5, \beta^{10}\} = \left\{\alpha, \alpha^2, \alpha^4, \alpha^8\right\}$ هي جميع جذور $m_5(x)$ وبهذا نرى أن $deg(m_5(x)) = 2$ وذلك من المبرهنة (**٥,٢,٤**). إذن، $m_5(x) = a_0 + a_1 x + a_2 x^2$. ونرى أن :

$$
\begin{aligned}
0 &= a_0 + a_1\beta^5 + a_2\beta^{10} \\
&= a_0(1000) + a_1(0110) + a_2(1110)
\end{aligned}
$$

وبحل هذا النظام نجد أن $a_0 = a_1 = a_2 = 1$. إذن، $m_5(x) = 1 + x + x^2$.

وبالأسلوب نفسه نستطيع إيجاد كثيرات الحدود الأصغرية لبقية عناصر الحقل $GF(2^4)$ المنشأ باستخدام $h(x) = 1 + x + x^4$ والجدول (**٥,٢**) يُبيّن ذلك.

الجدول (٥,٢). كثيرات الحدود الأصغرية لعناصر $GF(2^4)$.

كثيرات الحدود الأصغرية	عناصر $GF(2^4)$
x	0
$1 + x$	1
$1 + x + x^4$	$\beta, \beta^2, \beta^4, \beta^8$
$1 + x + x^2 + x^3 + x^4$	$\beta^3, \beta^6, \beta^9, \beta^{12}$
$1 + x + x^2$	β^5, β^{10}
$1 + x^3 + x^4$	$\beta^7, \beta^{11}, \beta^{13}, \beta^{14}$

▲

تمارين

(**٥,٢,٦**) تحقق من صواب الجدول (**٥,٢**) للحقل $GF(2^4)$.

(**٥,٢,٧**) جد كثيرة الحدود الأصغرية لكل من عناصر $GF(2^3)$ المنشأ باستخدام $p(x) = 1 + x + x^3$ (انظر التمرين (**٥,١,١٥**)).

(**٥,٢,٨**) جد كثيرة الحدود الأصغرية لكل من عناصر $GF(2^4)$ المنشأ باستخدام $p(x) = 1 + x^3 + x^4$ (انظر التمرين (**٥,١,١٥**)).

(**٥,٢,٩**) جد كثيرة الحدود الأصغرية لكل من عناصر $GF(2^5)$ المنشأ باستخدام $p(x) = 1 + x^2 + x^5$ (انظر التمرين (**٥,١,١٥**)).

(**٥,٢,١٠**) أثبت أن $1 + x + x^2 = (\beta^5 + x)(\beta^{10} + x)$ (استخدم الجدول (**٥,١**)).

(**٥,٢,١١**) أثبت أن $m_\alpha(x)$ كثيرة حدود بدائية إذا وفقط إذا كان α عنصراً بدائياً.

(٥,٣) شفرات هامينغ الدورية

Cyclic Hamming Codes

رأينا سابقاً أن شفرات هامينغ تتمتع بخصائص مهمة فهي شفرات تامة وتستطيع تصويب خطأ واحد وعملية فك التشفير سهلة. في هذا البند سنثبت وجود شفرة هامينغ دورية من الطول $n = 2^r - 1$ لكل $r \geq 2$ مما يؤدي إلى سهولة التشفير لهذه الشفرات (كشفرات دورية).

تتكون مصفوفة اختبار النوعية لشفرة هامينغ من الطول $n = 2^r - 1$ من عدد $2^r - 1$ صفاً من الكلمات غير الصفرية من الطول r. إذا كان β عنصراً بدائياً في الحقل $GF(2^r)$ فنجد من التعريف أن جميع قوى β مختلفة ولذلك يكون بمقدورنا إنشاء شفرة هامينغ من الطول $n = 2^r - 1$ بحيث تكون مصفوفة اختبار النوعية لها هي المصفوفة:

$$\begin{bmatrix} 1 \\ \beta \\ \beta^2 \\ \vdots \\ \beta^{2^r-2} \end{bmatrix}$$

لاحظ أن درجة H تساوي $(2^r - 1) \times r$. لاحظ أيضاً أنه إذا كانت $w = w_0 w_1 \cdots w_{n-1}$ كلمة مستقبلة فإن $wH = w_0\beta^0 + w_1\beta^1 + \cdots + w_{n-1}\beta^{n-1}$. وبهذا تكون w كلمة شفرة إذا وفقط إذا كانت β جذراً لكثيرة الحدود $w(x)$. إذن، استناداً إلى المبرهنة **(٥,٢,٢)** (ب) نجد أن $m_\beta(x)$ تقسم جميع كلمات الشفرة وهي كلمة شفرة بحد ذاتها. وبهذا تكون شفرة هامينغ دورية مولّدة بكثيرة الحدود $m_\beta(x)$ ونكون قد أثبتنا المبرهنة التالية :

مبرهنة (٥,٣,١)

أي كثيرة حدود بدائية من الدرجة r هي كثيرة حدود مولّدة لشفرة هامينغ الدورية من الطول $2^r - 1$. ■

مثال (٥,٣,٢)

لنفرض أن $r = 3$. عندئذ، $n = 2^3 - 1 = 7$. باستخدام $p(x) = 1 + x + x^3$ لإنشاء $GF(2^3)$ و $\beta \leftrightarrow 010$ كعنصر بدائي $(\beta^i \longleftrightarrow x^i (mod\, p(x)))$ نجد أن مصفوفة اختبار النوعية لشفرة هامينغ من الطول 7 هي :

$$\begin{bmatrix} 1 \\ \beta \\ \beta^2 \\ \beta^3 \\ \beta^4 \\ \beta^5 \\ \beta^6 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 111 \\ 101 \end{bmatrix}$$

وهي مصفوفة اختبار النوعية نفسها للشفرة الدورية المولّدة بكثيرة الحدود $p(x) = m_\beta(x)$. ▲

فك تشفير شفرة هامينغ الدورية أمر يسير، فإذا كانت كثيرة الحدود المولّدة هي كثيرة الحدود البدائية $m_\alpha(x)$ وكانت $w(x)$ هي الكلمة المستقبلة فنرى أن $w(x) = c(x) + e(x)$ حيث $c(x)$ كلمة شفرة و $w(\alpha) = e(\alpha)$. وبما أن وزن e يساوي 1 فنرى أن $e(\alpha) = \alpha^j$ حيث j هو موقع الإحداثي 1 في الكلمة e، وذلك باستخدام الترقيم $0,1,\cdots,n$ لمواقع إحداثيات e. إذن، كثيرة حدود الخطأ هي على الأرجح $e(x) = x^j$. وبهذا يكون $c(x) = w(x) + x^j$.

مثال (٥,٣,٣)

لنفرض أن الحقل $GF(2^3)$ أنشئ باستخدام $1 + x + x^3$. عندئذ، $m_1(x) = 1 + x + x^3$ هي كثيرة حدود مولّدة لشفرة هامينغ الدورية من الطول 7. لنفرض أن الكلمة المستقبلة هي $w(x) = 1 + x + x^3 + x^6$. حينئذ،

$$\begin{aligned} w(\beta) &= 1 + \beta^2 + \beta^3 + \beta^6 \\ &= 100 + 001 + 110 + 101 \\ &= 110 \\ &= \beta^3 \end{aligned}$$

إذن، $e(x) = x^3$ ويكون $c(x) = w(x) + x^3 = 1 + x^2 + x^6$. ▲

تمارين

(٥,٣,٤) جد مصفوفة اختبار النوعية لشفرة هامينغ الدورية من الطول 7 باستخدام $GF(2^3)$ المنشأ بكثيرة الحدود $1 + x + x^3$ حيث كثيرة الحدود المولّدة هي $m_3(x)$. وإذا كانت $w(x) = x + x^2 + x^4$ هي الكلمة المستقبلة فجد كلمة الشفرة $c(x)$ التي تكون على الأرجح قد أُرسلت.

(٥,٣,٥) أعد التمرين (٥,٣,٤) إذا استخدمت $p(x) = 1 + x^2 + x^3$ لإنشاء $GF(2^3)$ وكانت $m_1(x)$ هي كثيرة الحدود المولّدة.

(٥,٣,٦) أعد التمرين **(٥,٣,٤)** إذا استخدمت $p(x) = 1 + x^2 + x^3$ لإنشاء $GF(2^3)$ وكانت $m_3(x)$ هي كثيرة الحدود المولّدة.

(٥,٣,٧) أنشئ مصفوفة اختبار النوعية لشفرة هامينغ الدورية من الطول 15.

(٥,٣,٨) جد كثيرة حدود مولّدة لشفرة هامينغ الدورية من الطول 15 التي جذورها $1, \beta^7, \beta^5 \epsilon GF(2^4)$ (استخدمت $1 + x + x^4$ لإنشائه). أنشئ مصفوفة اختبار النوعية لهذه الشفرة. أثبت أن $c(x) \epsilon C$ إذا وفقط إذا كان $wt(c)$ زوجياً.

(٥,٣,٩) أثبت أن وزن كلمة شفرة من شفرة دورية يكون زوجياً إذا وفقط إذا كان $1 + x$ قاسماً لكثيرة الحدود المولّدة.

من المناسب التنويه هنا عن إمكانية استخلاص نتائج أعم مما حصلنا عليه في هذا البند. لتكن C شفرة دورية طولها n ولتكن $g(x)$ كثيرة حدودها المولّدة. لنفرض أن $\epsilon \alpha GF(2^r)$ جذر لكثيرة الحدود $g(x)$. عندئذ، $c(\alpha) = 0$ لكل $c(x) \epsilon C$. واستناداً إلى المبرهنة **(٥,٢,٢)** (ب) نرى أن $m_\alpha(x)$ تقسم $c(x)$. وبما أنه من الممكن دائماً كتابة $g(x)$ كحاصل ضرب كثيرات حدود أصغرية لعناصر من $GF(2^r)$ فنرى إمكانية استخدام ذلك لإنشاء مصفوفة اختبار النوعية وإيجاد خوارزمية لفك الشفرة C. سنناقش الحالة $g(x) = m_\beta(x) m_{\beta^3}(x)$ في البند **(٥,٤)**.

(٥,٤) شفرات BCH

BCH Codes

شفرات **بوسيه وتشودري وهوكنـــهام (Bose-Chaudhuri-Hocquengham)** أو اختصاراً شفرات BCH هي صنف مهم من الشفرات التي تصوّب عديدًا من الأخطاء. سنبدأ بإنشاء وفك تشفير شفرات خاصة من هذا الصنف تصوّب خطأين ونرجئ دراسة شفرات BCH العامة إلى وقت لاحق.

هناك سببان يجعلان شفرات BCH في غاية الأهمية، أولهما وجود خوارزمية سهلة نسبياً لفك تشفيرها والسبب الآخر هو الانتشار الواسع لهذه الشفرات. في واقع الأمر، لكل عددين صحيحين موجبين r و t حيث $t \leq 2^{r-1} - 1$ توجد شفرة BCH من الطول $n = 2^r - 1$ والبُعد $k \geq n - rt$ التي تصوّب أخطاء من النوع t.

شفرة BCH من الطول $2^r - 1$ التي تصوّب خطأين هي الشفرة الخطية الدورية المولّدة بكثيرة الحدود $g(x) = m_\beta(x)m_{\beta^3}(x)$ حيث β عنصر بدائي في الحقل $GF(2^r)$ ، $r \geq 4$. لاحظ أن $g(x)$ كثيرة حدود مولّدة لشفرة دورية ؛ لأن $n = 2^r - 1$ و $g(x)$ تقسم $1 + x^n$ (انظر المبرهنة (٥,٢,٢) (ج)).

مثال (٥,٤,١)

لنفرض أن $GF(2^4)$ هو الحقل المنشأ باستخدام $p(x) = 1 + x + x^4$ (انظر الجدول (٥,١)).

حينئذ، β عنصر بدائي و $m_1(x) = 1 + x + x^4$ و $m_3(x) = 1 + x + x^2 + x^3 + x^4$.

إذن،

$$g(x) = m_1(x)m_3(x) = 1 + x^4 + x^6 + x^7 + x^8$$

هي كثيرة حدود مولّدة لشفرة BCH من الطول 15 التي تصوّب خطأين. ▲

تمارين

(**٥,٤,٢**) شفرات BCH التي تصوّب خطأين معرّفة عندما يكون $r \geq 4$. ما هي الشفرة التي تولّدها $g(x) = m_1(x)m_3(x)$ في الحالة $r = 3$.

(**٥,٤,٣**) ليكن β عنصراً بدائياً في الحقل $GF(2^4)$ المنشأ باستخدام كثيرة الحدود غير القابلة للتحليل $p(x) = 1 + x^3 + x^4$. جد كثيرة حدود مولّدة $g(x)$ لشفرة BCH من الطول 15 التي تصوّب خطأين مُستخدماً هذا التمثيل للحقل $GF(2^4)$. أي جد $g(x) = m_1(x)m_3(x)$ (انظر التمرين (٥,١,١٥)).

(٥,٤,٤) استخدم كثيرة الحدود غير القابلة للتحليل $1 + x^2 + x^5$ لإنشاء $GF(2^5)$ ثم جد كثيرة حدود مولّدة لشفرة BCH من الطول 31 التي تصوّب خطأين (انظر التمرين (**٥,١,١٥**)).

تمهيدية (٥,٤,٥)

المصفوفة التالية H هي مصفوفة اختبار النوعية لشفرة BCH من الطول $2^r - 1$ التي تصوّب خطأين حيث β عنصر بدائي في الحقل $GF(2^r)$ و $g(x) = m_1(x)m_3(x)$ كثيرة الحدود المولّدة.

$$H = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \vdots \\ \beta^i & \beta^{3i} \\ \vdots & \vdots \\ \beta^{2^r-2} & \beta^{3(2^r-2)} \end{bmatrix}$$

البرهان

بما أن $\beta^i \epsilon GF(2^r)$ فهي تمثل كلمة طولها r ونرى أن H مصفوفة من الدرجة $(2^r - 2) \times (2r)$. وبما أن $deg(m_1(x)) = r = deg(m_3(x))$ فنجد أن درجة $g(x) = m_1(x)m_3(x)$ تساوي $2r$. وبهذا يكون بُعد الشفرة هو $n - 2r = 2^r - 1 - 2r$.

سنترك إثبات أن درجة $m_3(x)$ تساوي r للتمرين (**٥,٤,٩**). ■

على سبيل المثال، إذا استخدمنا الحقل $GF(2^4)$ المنشأ في الجدول (**٥,١**) باستخدام كثيرة الحدود البدائية $p(x) = 1 + x + x^4$ لإنشاء شفرة BCH لتصويب خطأين C_{15} نجد أن C_{15} هي الشفرة الخطية التي لها مصفوفة اختبار النوعية H من الدرجة 15×8 وكثيرة الحدود المولّدة $m_1(x)m_3(x)$ (انظر الجدول (**٥,٣**)).

الجدول (٥,٣). مصفوفة اختبار النوعية للشفرة C_{15}.

$$\begin{bmatrix} 1 & 1 \\ \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^9 \\ \beta^4 & \beta^{12} \\ \beta^5 & 1 \\ \beta^6 & \beta^3 \\ \beta^7 & \beta^6 \\ \beta^8 & \beta^9 \\ \beta^9 & \beta^{12} \\ \beta^{10} & 1 \\ \beta^{11} & \beta^3 \\ \beta^{12} & \beta^6 \\ \beta^{13} & \beta^9 \\ \beta^{14} & \beta^{12} \end{bmatrix} \longleftrightarrow \begin{bmatrix} 1000 & 1000 \\ 0100 & 0001 \\ 0010 & 0011 \\ 0001 & 0101 \\ 1100 & 1111 \\ 0110 & 1000 \\ 0011 & 0001 \\ 1101 & 0011 \\ 1010 & 0101 \\ 0101 & 1111 \\ 1110 & 1000 \\ 0111 & 0001 \\ 1111 & 0011 \\ 1011 & 0101 \\ 1001 & 1111 \end{bmatrix} = H$$

مبرهنة (٥,٤,٦)

لكل عدد صحيح $r \geq 4$ توجد شفرة BCH من الطول $n = 2^r - 1$ والبُعد $k = 2^r - 2r - 1$ التي تصوّب خطأين ومسافتها تساوي 5 وكثيرة حدودها المولّدة هي $m_1(x)m_3(x)$.

البرهان

إثبات أن المسافة تساوي 5 نحصل عليه من كون الشفرة تصوّب خطأين ومن ثم فإن مسافتها على الأقل 5. ومن تعريف مصفوفة اختبار النوعية نرى أن $n = 2^r - 1$. وبملاحظة أن درجة كل من $m_1(x)$ و $m_3(x)$ تساوي r نجد أن درجة $g(x)$ تساوي $n - k = 2r$ وبهذا يكون $k = 2^r - 2r - 1$. ■

تمارين

(٥,٤,٧) أثبت أن أعمدة مصفوفة اختبار النوعية للشفرة C_{15} المبينة في الجدول **(٥,٣)** مُستقلة خطياً ومن ثم بُعد C_{15} هو $k = 7$.

(**٥,٤,٨**) استخدم مصفوفة اختبار النوعية لإثبات أن مسافة C_{15} هي $d = 5$.

(**٥,٤,٩**) إذا كان β عنصراً بدائياً في الحقل $GF(2^r)$ حيث $r > 2$ فأثبت أن:

$$\left|\left\{\beta^{2^i}: 0 \leq i \leq r-1\right\}\right| = r$$ وأن

$$\left|\left\{(\beta^3)^{2^i}: 0 \leq i \leq r-1\right\}\right| = r$$

واستنتج أن درجة كل من $m_1(x)$ و $m_3(x)$ تساوي r.

(**٥,٤,١٠**) بيّن ما إذا كانت الكلمات التالية من الطول 15 هي كلمات تنتمي إلى الشفرة C_{15} حيث $g(x) = 1 + x^4 + x^6 + x^7 + x^8$.

(أ) 011001011000010 (ب) 000111010000110

(ج) 011100000010001 (د) 111111111111111.

(**٥,٥**) فك تشفير شفرة BCH التي تصوّب خطأين

Decoding 2 Error-Correcting BCH Code

نقدم خوارزمية لفك تشفير BCH التي تصوّب خطأين المقدمة في البند السابق.

في هذا البند نطابق الكلمة الثنائية من الطول r مع قوة β المقابلة لها. مصفوفة اختبار النوعية لشفرة BCH التي تصوّب خطأين من النوع $(2^r - 1, 2^r - 2r - 1, 5)$ والتي كثيرة حدودها المولّدة $g(x) = m_1(x)m_3(x)$ هي المصفوفة H المقدمة في التمهيدية (**٥,٤,٥**).

لنفرض أن w هي الكلمة المستقبلة وأن $w(x) \leftrightarrow w$. عندئذ، تناذر w هو:

$$wH = [w(\beta), w(\beta^3)] = [s_1, s_3]$$

حيث s_1 و s_3 كلمتان طول كل منهما يساوي r.

إذا لم يحدث خطأ في الإرسال فنرى أن التناذر $wH = 0$ ويكون $s_1 = s_3 = 0$.

إذا وقع خطأ واحد فقط أثناء عملية الإرسال فإن كثيرة حدود الخطأ هي $e(x) = x^i$ ونرى أن $wH = eH = [e(\beta), e(\beta^3)] = [\beta^i, \beta^{3i}] = [s_1, s_3]$.

وبهذا يكون $s_1^3 = s_3$. أما إذا وقع خطآن أثناء عملية الإرسال في الموقعين i و j حيث $i \neq j$ فنجد أن $e(x) = x^i + x^j$ وأن $wH = eH = [e(\beta), e(\beta^3)] = [s_1, s_3]$.

وبهذا نرى أن تناذر wH هو $wH = [s_1, s_3] = [\beta^i + \beta^j, \beta^{3i} + \beta^{3j}]$.

ونحصل على نظام المعادلات:

$$\beta^i + \beta^j = s_1$$
$$\beta^{3i} + \beta^{3j} = s_3$$

ولكن لدينا التحليل:

$$(\beta^i + \beta^j)(\beta^{2i} + \beta^{i+j} + \beta^{2j}) = \beta^{3i} + \beta^{3j}$$

و

$$s_1^2 = (\beta^i + \beta^j)^2 = \beta^{2i} + \beta^{2j}$$

إذن،

$$\begin{aligned} s_3 &= \beta^{3i} + \beta^{3j} \\ &= (\beta^i + \beta^j)(\beta^{2i} + \beta^{2j} + \beta^{i+j}) \\ &= s_1(s_1^2 + \beta^{i+j}) \end{aligned}$$

وبهذا نرى أن:

$$\frac{s_3}{s_1} + s_1^2 = \beta^{i+j}.$$

ولكن β^i و β^j جذرا المعادلة التربيعية:

$$x^2 + (\beta^i + \beta^j)x + \beta^{i+j} = 0.$$

ومن ثم فهما جذرا المعادلة:

$$x^2 + s_1 x \left(\frac{s_3}{s_1} + s_1^2\right) = 0.$$

وعليه نستطيع إيجاد موقعي الخطأين بإيجاد جذري المعادلة. كثيرة الحدود في الطرف الأيسر للمعادلة تُسمى **كثيرة حدود تعيين الخطأ (Error Locator Polynomial)**.

مثال (٥,٥,١)

لنفــــرض أن $w \leftrightarrow w(x)$ كلمـــــة مســــتقبلة بتنــــاذر $s_1 = 0111 = w(\beta)$ و $s_3 = 1010 = w(\beta^3)$ حيث تم تشفير w باستخدام C_{15}. باستخدام الجدول (٥,١) نجد أن $s_1 \leftrightarrow \beta^{11}$ و $s_3 \leftrightarrow \beta^8$. عندئذ،

$$\begin{aligned}\frac{s_3}{s_1} + s_1^2 &= \beta^8\beta^{-11} + \beta^{22}\\ &= \beta^{12} + \beta^7\\ &= \beta^2\end{aligned}$$

وعليه نجد أن جذري كثيرة الحدود $x^2 + \beta^{11}x + \beta^2$ هما β^4 و β^{13}. وبهذا نستطيع تحديد موقعي الخطأ فيكونا الموقعين 4 و 13 (أي أن $e(x) = x^4 + x^{13}$). إذن، نمط الخطأ الأرجح هو:

.000010000000010 ▲

تمارين

(٥,٥,٢) أثبت أن β^4 و β^{13} هما بالفعل جذرا كثيرة الحدود $x^2 + \beta^{11}x + \beta^2 = 0$.

بيّن أيضاً أن مجموع الصفين 4 و 13 من المصفوفة H المبينة في الجدول (٥,٣) هو $[s_1, s_3]$.

(٥,٥,٣) جد جذور كثيرات الحدود التالية في الحقل $GF(2^4)$ إن أمكن ذلك (استخدم الجدول (٥,١)):

(أ) $x^2 + \beta^4x + \beta^{13}$ (ب) $x^2 + \beta^7x + \beta^2$

(ج) $x^2 + \beta^2x + \beta^5$ (د) $x^2 + \beta^6$

(هـ) $x^2 + \beta^2x$ (و) $x^2 + x + \beta^8$.

نقدم الآن خوارزمية لطريقة الاحتمالية القصوى غير التامة IMLD لفك تشفير شفرات BCH التي تصوّب خطأين. لنفرض أن w كلمة مستقبلة. الخوارزمية تتوقف في اللحظة التي يتم بها تحديد نمط الخطأ.

خوارزمية (٥,٥,٤) [فك تشفير شفرة BCH التي تصوّب خطأين]

لنفرض أن كثيرة الحدود المولّدة هي $m_1(x)m_3(x)$.

(١) احسب التناذر $wH = [s_1, s_3] = [w(\beta), w(\beta^3)]$.

(٢) إذا كان $s_1 = s_3 = 0$ فنستنتج عدم وقوع أخطاء ونخلص إلى أن $c = w$ هي كلمة الشفرة المرسلة.

(٣) إذا كان $s_1 = 0$ و $s_3 \neq 0$ فنطلب إعادة الإرسال.

(٤) إذا كان $s_1^3 = s_3$ فيتم تصويب خطأ واحد فقط في الموقع i حيث $s_1 = \beta^i$.

(٥) كوّن المعادلة التربيعية $x^2 + s_1 x + \frac{s_3}{s_1} + s_1^2 = 0$. $(*)$

(٦) إذا كان للمعادلة $(*)$ جذرين مختلفين β^i و β^j فنصوّب خطئين في الموقعين i و j.

(٧) إذا لم يكن للمعادلة $(*)$ جذرين مختلفين في الحقل $GF(2^r)$ فنخلص إلى وقوع ثلاثة أخطاء على الأقل أثناء الارسال ونطلب إعادة الإرسال.

جميع الأمثلة والتمارين التي سنناقشها تستخدم الشفرة C_{15} حيث مصفوفة اختبار النوعية مبينة في الجدول (٥,٣) وكثيرة حدودها المولّدة $g(x)$ هي المقدمة في المثال (٥,٤,١).

مثال (٥,٥,٥)

لنفرض أن w كلمة مستقبلة وأن التناذر هو:

$$wH = 01111010 \leftrightarrow [\beta^{11}, \beta^8].$$

عندئذ، $s_1^3 = (\beta^{11})^3 = \beta^{33} = \beta^3 \neq \beta^8 = s_3$.

في هذه الحالة تكون المعادلة $(*)$ هي $x^2 + \beta^{11}x + \beta^2 = 0$ وهي المعادلة المبينة في المثال (٥,٥,١). لهذه المعادلة جذران مختلفان هما β^4 و β^{13}. إذن، نستطيع تصويب خطأين في الموقعين $i = 4$ و $j = 13$. أي أن نمط الخطأ الأرجح هو:

$u = 000010000000010$ وأن $e(x) = x^4 + x^{13}$ هي كثيرة حدود الخطأ. ▲

مثال (٥,٥,٦)

لنفرض أن التناذر هو $wH = [w(\beta), w(\beta^3)] = [\beta^3, \beta^9]$. عندئذ، $s_1^3 = (\beta^3)^3 = \beta^9 = s_3$. إذن، نستنتج وقوع خطأ واحد على الأرجح في الموقع $i = 3$. ويكون نمط الخطأ الأرجح $u = 000010000000000$ و $e(x) = x^3$ هي كثيرة حدود الخطأ. ▲

مثال (٥,٥,٧)

لنفرض أن $w = 110111101011000$ كلمة مُستقبلة. عندئذ، التناذر هو:

$$wH = 01110110 \leftrightarrow [\beta^{11}, \beta^5] = [s_1, s_3].$$

الآن، $s_1^3 = (\beta^{11})^3 = \beta^{33} = \beta^3 \neq s_3 = \beta^5$. لايجاد المعادلة التربيعية (*) يلزمنا حساب:

$$\begin{aligned}\frac{s_3}{s_1} + s_1^2 &= \beta^5\beta^{-11} + (\beta^{11})^2 \\ &= \beta^9 + \beta^7 \\ &\leftrightarrow 0101 + 1101 \\ &= 1000 \\ &\leftrightarrow \beta^0\end{aligned}$$

ونرى أن المعادلة (*) في هذه الحالة هي $x^2 + \beta^{11}x + \beta^0 = 0$. وبتجريب عناصر $GF(2^4)$ لإيجاد الجذور المحتملة نجد أن $x = \beta^7$ يحقق:

$$\begin{aligned}(\beta^7)^2 + \beta^{11}\beta^7 + \beta^0 &= \beta^{14} + \beta^3 + \beta^0 \\ &\leftrightarrow 1001 + 0001 + 1000 \\ &= 0000\end{aligned}$$

وبملاحظة أن $\beta^{15} = 1 = \beta^7\beta^i$ نجد أن $\beta^i = \beta^8$ هو الجذر الآخر. إذن، يمكن تصويب خطأين في الموقعين $i = 7$ و $j = 8$ ويكون نمط الخطأ هو $u = 000000011000000$ ونخلص إلى أن $v = w + u = 110111110011000$ هي الكلمة المرسلة. ▲

مثال (٥,٥,٨)

لنفرض أنه أثناء عملية إرسال كلمة من كلمات الشفرة C_{15} قد وقعت أخطاء في المواقع 2 و 6 و 12. عندئذ، يكون التناذر wH هو مجموع الصفوف 2 ، 6 ، 12 من المصفوفة H حيث w هي الكلمة المستقبلة. حينئذ،

$$wH = 00100011 + 00110001 + 11110011$$
$$= 11100001 \leftrightarrow [\beta^{10}, \beta^{3}] = [s_1, s_3]$$

الآن ، $s_1^3 = (\beta^{10})^3 = \beta^{30} = 1 \neq \beta^3 = s_3$. وعليه فإن:

$$\frac{s_3}{s_1} + s_1^2 = \beta^3\beta^{-10} + \beta^{20} = \beta^8 + \beta^5$$
$$\leftrightarrow 1010 + 0110 = 1100 \leftrightarrow \beta^4$$

ومن ثم فالمعادلة التربيعية هي $x^2 + \beta^{10}x + \beta^4 = 0$.

وبتجريب جميع عناصر $GF(2^4)$ نخلص إلى عدم وجود جذور لهذه المعادلة في الحقل $GF(2^4)$. إذن، تستنتج طريقة IMLD لفك تشفير C_{15} إلى وقوع ثلاثة أخطاء على الأقل أثناء الإرسال ومن ثم نطلب إعادة الإرسال. ▲

تمارين

(٥,٥,٩) تم تشفير رسائل باستخدام C_{15}. إذا كانت w هي الكلمة المستقبلة وكان wH تناذرها فحدّد مواقع الأخطاء التي حدثت أثناء الارسال (إن أمكنك ذلك).

(أ) 0100 0101 (ب) 1110 1000

(ج) 1100 1101 (د) 0100 0000

(هـ) 0000 0100 (و) 1010 0100

(ز) 0011 1101 (ح) 0000 0000.

(٥,٥,١٠) الشفرة هي C_{15}. فُك تشفير كل من الكلمات المستقبلة w التالية إن أمكن ذلك.

(أ) 11000 00000 00000 (ب) 00001 00001 00001

(ج) 01000 10101 00000 (د) 11001 11001 11000

(هـ) 11001 11001 00000 (و) 11100 00000 00001

(ز) 10111 00000 00000 (ح) 10101 00101 10001

(ط) 01000 01000 00000 (ي) 01010 10010 11000

(ك) 11011 10111 01100 (ل) 10111 00000 01000

(م) 11100 10110 00000 (ن) 00011 10100 00110.

الفصل السادس

شفرات ريد وسولومن
Reed-Solomon Codes

(٦,١) شفرات على $GF(2^r)$
Codes Over $GF(2^r)$

شفرات ريد وسولومن هي بلا شك أكثر الشفرات استخداماً في التطبيقات العملية، فهي التي تستخدم حالياً من قبل وكالة الفضاء الأمريكية (NASA) ووكالة الفضاء الأوروبية. كما أن الشفرات التي يتم اختيارها لاستخدامها على الأقراص الممغنطة تنتمي إلى عائلة شفرات ريد وسولومن.

درسنا في البند السابق بالتفصيل شفرات BCH الثنائية التي تصوّب خطأين. في الحقيقة شفرات ريد وسولومن هي شفرات BCH ولكنها ليست ثنائية. قد يبدو هذا غريباً للوهلة الأولى حيث عمليات الإرسال تتم عبر قنوات اتصال ثنائية. سنُبيّن في وقت لاحق أن لهذه الشفرات تمثيلاً ثنائياً.

لنفرض أن $GF(2^r)[x]$ هي مجموعة جميع كثيرات الحدود التي معاملاتها تنتمي إلى الحقل $GF(2^r)$. لاحظ أن هذه المجموعة تحتوي مجموعة كثيرات الحدود ذات المعاملات الثنائية $K[x]$ حيث $K = GF(2) = \{0,1\}$. إذا كانت C شفرة خطية على

$GF(2^r)$ من الطول n وكانت $c\epsilon C$ فسوف نطابق c مع كثيرة حدود $c(x)\epsilon GF(2^r)[x]$ حيث $deg(c(x)) < n$.

لقد سبق وعرفنا الشفرات الدورية من الطول n بدلالة جذور كثيرات الحدود المقابلة. على سبيل المثال، عرفنا شفرة BCH من الطول $n = 2^r - 1$ التي تصوّب خطأين على النحو التالي: $c(x)\epsilon C_K$ إذا وفقط إذا كانت $\beta^1, \beta^2, \beta^3, \beta^4$ هي جميع جذور كثيرة الحدود $c(x)$ حيث $c(x)\epsilon K[x]$ و $deg(c(x)) < n$ و β عنصر بدائي في الحقل $GF(2^r)$. وفي هذه الحالة تكون $g_K(x) = m_1(x)m_3(x)$ هي كثيرة الحدود المولّدة لهذه الشفرة الدورية وتكون $c(x)\epsilon C_K$ إذا وفقط إذا كان $c(x) = a(x)g_K(x)$.

من الممكن تعميم هذه الشفرة إلى شفرة على الحقل $GF(2^r)$ بأخذ $c(x)\epsilon GF(2^r)[x]$ عوضاً عن $c(x)\epsilon K[x]$. وبهذا يكون $c(x)\epsilon C$ إذا وفقط إذا كانت $\{\beta^1, \beta^2, \beta^3, \beta^4\}$ هي جميع جذور $c(x)$. ولكون $x + \beta$ ، $x + \beta^2$ ، $x + \beta^3$ ، $x + \beta^4$ هي كثيرات حدود تنتمي إلى $GF(2^r)[x]$ نرى أن $c(x)\epsilon C$ إذا وفقط إذا كانت كثيرة الحدود $g(x) = (x + \beta)(x + \beta^2)(x + \beta^3)(x + \beta^4)$ تقسم كثيرة الحدود $c(x)$.

الشفرة الثنائية C_K المعرّفة في الفقرة الثانية من هذه الصفحة هي شفرة BCH وأما الشفرة C على الحقل $GF(2^r)$ فهي إحدى شفرات ريد وسولومن. لاحظ أن C_K شفرة جزئية من C. بصورة عامة، الشفرة C_K هي شفرة على **حقل جزئي وشفرة جزئية (Subfield Subcode)** من C ؛ لأن $C_K \subseteq C$ وجميع إحداثيات كلمات الشفرة C_K تنتمي إلى الحقل الجزئي K من $GF(2^r)$. أي أن $C_K = C \cap K^n$.

كل من الشفرتين C_K و C دورية ؛ لأنه إذا كانت $c(x)\epsilon C$ فنجد أن $c(x) \equiv xc(x)(mod 1 + x^n)\epsilon C$، وذلك باستخدام خوارزمية القسمة وكون β^i جذراً لكل من $1 + x^n$ و $xc(x)$. في الحقيقة، ليس بالأمر الصعب إثبات أنه إذا كانت $g(x)$

كثيرة حدود مولّدة لشفرة خطية دورية من الطول $2^r - 1$ على الحقل $GF(2^r)$ فنرى أن كثيرة الحدود $g_K(x)$ المولّدة للشفرة الجزئية الثنائية التي هي شفرة على الحقل الجزئي، هي كثيرة الحدود التي مجموع جذورها هي أصغر مجموعة R تحقق:

(أ) $g(\alpha) = 0 \Rightarrow \alpha \epsilon R$ (ب) $\epsilon \alpha R \Rightarrow \alpha^2 \epsilon R$.

مما سبق نحصل على المبرهنة التالية:

مبرهنة (٦,١,١)

إذا كانت $\alpha_1, \alpha_2, \cdots, \alpha_t$ عناصر غير صفرية مختلفة في الحقل $GF(2^r)$ فإن $g(x) = (\alpha_1 + x)(\alpha_2 + x) \cdots (\alpha_t + x)$ تولّد شفرة خطية دورية من الطول $2^r - 1$ على الحقل $GF(2^r)$.

مثال (٦,١,٢)

لنفرض أن $F = GF(2^4)$ الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**)). عندئذ، $g(x) = (\beta + x)(\beta^2 + x) = \beta^3 + \beta^5 x + x^2$ تولّد شفرة خطية دورية C من الطول 15 على الحقل F. كلمة الشفرة المقابلة لكثيرة الحدود $g(x)$ هي $\beta^3\beta^5 1000000000000$. أيضاً، $g_K(x) = 1 + x + x^4 \leftrightarrow 110010000000000$ تولّد الشفرة الدورية الثنائية التي هي شفرة على الحقل الجزئي وشفرة جزئية من الشفرة C. ولإثبات ذلك نجد مجموعة جذور R فنرى أن $\beta, \beta^2 \epsilon R$ (استناداً إلى (أ))، واستناداً إلى الفقرة (ب) نرى أن $(\beta^2)^2 = \beta^4 \epsilon R$ وأن $(\beta^4)^2 = \beta^8 \epsilon R$. إذن، $R = \{\beta, \beta^2, \beta^4, \beta^8\}$ وبهذا تكون $g_K(x) = (\beta^4 + x)(\beta^8 + x) g(x)$. ▲

نقدم فيما يلي بعض الخصائص الأساسية للشفرات الدورية على الحقل $GF(2^r)$.

مبرهنة (٦,١,٣)

لتكن C شفرة خطية دورية من الطول n على الحقل $GF(2^r)$. عندئذ، يمكن كتابة أي كلمة شفرة $c(x)$ بطريقة وحيدة كحاصل ضرب $m(x)g(x)$ حيث $m(x) \epsilon GF(2^r)[x]$

درجتها أصغر من $n - deg(g(x))$. أيضاً، $g(x)$ تقسم $f(x)$ إذا وفقط إذا كانت $f(x)$ كلمة شفرة و $g(x)$ تقسم $1 + x^n$.

نتيجة (٦,١,٤)

لتكن $g(x)$ كثيرة حدود درجتها $n - k$. إذا ولّدت $g(x)$ شفرة خطية دورية C على الحقل $GF(2^r)$ من الطول $n = 2^r - 1$ والبُعد k فإن:

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

مصفوفة مولّدة للشفرة C وعدد كلمات الشفرة C يساوي $(2^r)^k$.

ملحوظة

نحصل على $|C| = 2^{rk}$ من المبرهنة (**٦,١,٣**)؛ وذلك لأن جميع كثيرات الحدود $m(x)\epsilon GF(2^r)[x]$ التي درجة كل منها أصغر من k تقابل كلمات شفرة مختلفة $m(x)g(x)$. ولكن عدد كثيرات الحدود $m(x)$ يساوي 2^{rk}؛ لأن كلاً من معاملات $m(x)$ وعددها k هو أحد عناصر الحقل والتي عددها 2^r.

مثال (٦,١,٥)

لنفرض أن $GF(2^3)$ الحقل المنشأ باستخدام $1 + x + x^3$ وأن العنصر البدائي المستخدم هو β. ولنفرض أن $g(x) = (\beta + x)(\beta^2 + x) = \beta^3 + \beta^4 x + x^2$. حينئذ، $g(x)$ تولّد شفرة خطية دورية C على الحقل $GF(2^3)$ من الطول 7. مصفوفة مولّدة للشفرة C هي:

$$G = \begin{bmatrix} \beta^3 & \beta^4 & 1 & 0 & 0 & 0 & 0 \\ 0 & \beta^3 & \beta^4 & 1 & 0 & 0 & 0 \\ 0 & 0 & \beta^3 & \beta^4 & 1 & 0 & 0 \\ 0 & 0 & 0 & \beta^3 & \beta^4 & 1 & 0 \\ 0 & 0 & 0 & 0 & \beta^3 & \beta^4 & 1 \end{bmatrix}$$

عـدد كلمـات الشـفرة C يسـاوي 8^5. وكلمـة الشـفرة المقابلـة لكـثيرة الحـدود $m(x) = 1 + \beta x + \beta^3 x^4$ هي $m = 1\beta 00\beta^3$. فمثلاً ،

$.m(x)g(x) \leftrightarrow mG = \beta^3 0 \beta^4 \beta \beta^6 1 \beta^3$ ▲

تمارين

(**٦,١,٦**) ليكن $GF(2^3)$ الحقل المنشأ باستخدام كثيرة الحدود $x^3 + x + 1$. ولنفرض أن $g(x) = (1 + x)(\beta + x)$ تولّد الشفرة C من الطول 7 على الحقل $GF(2^3)$.

(أ) ما هو عدد كلمات الشفرة C ؟

(ب) استخدم النتيجة (**٦,١,٤**) لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) استخدم G لتشفير كل من الرسائل التالية :

(i) $.m(x) = 1 + \beta^6 x$

(ii) $.m(x) = \beta^4 x^4$

(iii) $.m(x) = 1 + x + x^2$

(د) جد كثيرة حدود مولّدة $g_K(x)$ للشفرة الدورية الثنائية التي هي شفرة على حقل جزئي وشفرة جزئية.

(**٦,١,٧**) ليكن $GF(2^4)$ الحقل المنشأ باستخدام كثيرة الحدود $x^4 + x + 1$. ولتكن $g(x) = (\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)$ كثيرة الحدود المولّدة للشفرة الخطية الدورية C على الحقل المنشأ $GF(2^4)$ من الطول 15.

(أ) ما هو عدد كلمات الشفرة C ؟

(ب) استخدم النتيجة (**٦,١,٤**) لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) استخدم G لتشفير كل من الرسائل التالية :

(i) $.m(x) = 1 + \beta^7 x^{10}$

(ii) $.m(x) = \beta^2 x + x^2$

.$m(x) = 1 + x + x^2$ (iii)

(د) جد كثيرة الحدود $g_K(x)$ المولّدة للشفرة الدورية الثنائية التي هي شفرة على حقل جزئي وشفرة جزئية. جد $m(x)$ التي تحقق $g_K(x) = m(x)g(x)$.

(٦,٢) شفرات ريد وسولومن

Reed-Solomon Codes

وجدنا في البند (٦,١) مولّدات للشفرة الخطية الدورية على الحقل $GF(2^r)$ ولكننا لم نتطرق إلى كفاءة هذه الشفرات لتصويب الأخطاء والتي ندرسها في هذا البند. كما أننا سنعرف شفرات ريد وسولومن وننوّه أن معظم النتائج التي نحصل عليها لهذه الشفرات يمكن استخدامها مباشرة لشفرات BCH ؛ لأن الأخيرة هي شفرة على حقل جزئي وشفرة جزئية. نبدأ بالتمهيدية التالية :

تمهيدية (٦,٢,١)

لنفرض أن $\alpha_1, \alpha_2, \cdots, \alpha_t$ عناصر غير صفرية في الحقل $GF(2^r)$. عندئذ ،

$$det\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{t-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_t & \alpha_t^2 & \cdots & \alpha_t^{t-1} \end{bmatrix} = \prod_{1\le j<i\le t} (\alpha_i + \alpha_j)$$

البرهان

إذا وجد عنصران $\alpha_i = \alpha_j$ حيث $i \neq j$ فتحتوي المصفوفة على صفين متساويين وتكون قيمة المحدد تساوي صفراً. إذن ، لكل $t \ge i > j \ge 1$ يكون $(\alpha_i + \alpha_j)$ قاسماً لقيمة المحدد وبهذا نرى أن $\prod_{1\le j<i\le t}(\alpha_i + \alpha_j)$ يقسم قيمة المحدد.

ولكون كل من طرفي المعادلة هو كثيرة حدود في $\alpha_1, \cdots, \alpha_t$ ولهما الدرجة نفسها نجد أنهما يختلفان بقاسم مشترك واحد على الأكثر. هذا القاسم المشترك هو 1 حيث نرى ذلك بمقارنة معاملات $\prod_{i=1}^{t} \alpha_i^{i-1}$ في الطرفين. ■

مثال (٦,٢,٢)

باستخدام التمهيدية (٦,٢,١) والحقل $GF(2^r)$ المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (٥,١)) نجد أن:

$$det \begin{bmatrix} 1 & \beta^2 & \beta^4 \\ 1 & \beta^7 & \beta^{14} \\ 1 & \beta^{10} & \beta^5 \end{bmatrix} = (\beta^7 + \beta^2)(\beta^{10} + \beta^2)(\beta^{10} + \beta^7)$$
$$= \beta^{12} \cdot \beta^4 \cdot \beta^6$$
$$= \beta^7$$

▲

تمرين

(٦,٢,٣) استخدم التمهيدية **(٦,٢,١)** لإيجاد قيمة المحدد المُبيّن بافتراض أن β عنصر بدائي في الحقل $GF(2^4)$ المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (٥,١)).

(أ) $.det \begin{bmatrix} 1 & \beta^2 & \beta^2 \\ 1 & \beta^4 & \beta^8 \\ 1 & \beta^7 & \beta^{14} \end{bmatrix}$

(ب) $.det \begin{bmatrix} 1 & \beta^2 & \beta^4 & \beta^6 \\ 1 & \beta^3 & \beta^6 & \beta^9 \\ 1 & \beta^5 & \beta^{10} & 1 \\ 1 & \beta^8 & \beta^1 & \beta^9 \end{bmatrix}$

(ج) $.det \begin{bmatrix} 1 & \beta^3 \\ 1 & \beta^7 \end{bmatrix}$

المبرهنة التالية هي المبرهنة الرئيسة لشفرات BCH العامة ومع أن الصيغة المقدمة ليست الصيغة العامة إلا أنها تفي بالغرض عند تطبيقها على شفرات ريد وسولومن.

مبرهنة (٦,٢,٤)

لتكن $g(x) = (\beta^{m+1} + x)(\beta^{m+2} + x) \cdots (\beta^{m+\delta-1} + x)$ كثيرة الحدود المولّدة للشفرة الخطية الدورية C على الحقل $GF(2^r)$ من الطول $n = 2^r - 1$ حيث β عنصر بدائي في الحقل $GF(2^r)$ وحيث m عدد صحيح موجب. حينئذ، $d(C) \geq \delta$.

البرهان

بما أن β^{m+i} جذر لكثيرة الحدود $g(x)$ لكل $1 \le i \le \delta - 1$ نرى أن أعمدة المصفوفة:

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta^{m+1} & \beta^{m+2} & \cdots & \beta^{m+\delta-1} \\ (\beta^{m+1})^2 & (\beta^{m+2})^2 & \cdots & (\beta^{m+\delta-1})^2 \\ \vdots & \vdots & & \vdots \\ (\beta^{m+1})^{n-1} & (\beta^{m+2})^{n-1} & \cdots & (\beta^{m+\delta-1})^{n-1} \end{bmatrix}$$

تولّد $C^{\perp}$. لاحظ أن أي تركيب خطي لأي $\delta - 1$ من صفوف هذه المصفوفة لا يمكن أن يكون صفراً حيث يمكن التحقق من ذلك بايجاد قيمة محدد مصفوفة جزئية عدد صفوفها $\delta - 1$. على سبيل المثال:

$$det\begin{bmatrix} (\beta^{m+1})^{j_1} & \cdots & (\beta^{m+1})^{j_1} \\ (\beta^{m+1})^{j_2} & \cdots & (\beta^{m+1})^{j_2} \\ \vdots & & \vdots \\ (\beta^{m+1})^{j_{\delta-1}} & \cdots & (\beta^{m+1})^{j_{\delta-1}} \end{bmatrix}$$

$$= \beta^{(m+1)(j_1+j_1+\cdots+j_{\delta-1})}\begin{bmatrix} 1 & \beta^{j_1} & (\beta^{j_1})^{\delta-2} \\ 1 & \beta^{j_2} & (\beta^{j_2})^{\delta-2} \\ \vdots & & \\ 1 & \beta^{j_{\delta-1}} & (\beta^{j_{\delta-1}})^{\delta-2} \end{bmatrix}$$

$$= \beta^{(m+1)(j_1+j_1+\cdots+j_{\delta-1})} \prod_{1 \le y \le x \le \delta-1} (\beta^{j_x} + \beta^{j_y})$$

وقيمة هذا المحدد لا تساوي صفراً؛ لأن رتبة β تساوي $n = 2^r - 1$ وأن $1 \le j_1 < j_1 < \cdots < j_{\delta-1} \le n - 1$.

وبهذا نرى عدم وجود تركيب خطي من صفوف عددها أصغر من أو يساوي $\delta - 1$ قيمته تساوي صفراً. ومن ذلك نجد استناداً إلى المبرهنة (**٢,٩,١**) أن $d(c) \ge \delta$. وبملاحظة أن أعمدة H مُستقلة خطياً نخلص إلى أن H مصفوفة اختبار النوعية للشفرة C. ■

ملحوظة

تبقى المبرهنة صحيحة لأي شفرة ثنائية خطية دورية من الطول $2^r - 1$ بحيث تكون $\beta^{m+1}, \cdots, \beta^{m+\delta-1}$ من ضمن جذور كثيرة حدودها المولّدة. تُسمى هذه الشفرات الثنائية، **شفرات BCH البدائية (Primitive BCH Codes)** وتُسمى δ، **المسافة المعتمدة (Designed Distance)** لهذه الشفرة. وبملاحظة أن هذه الشفرات هي شفرات ثنائية على حقول جزئية وشفرات جزئية $C_K \subset C$ من شفرات ريد وسولومن C فنرى أن $d(C_K) \geq \delta$ مُحققة أيضاً لهذه الشفرات.

تُعرف شفرة ريد وسولومن الثنائية $RS(2^r, \delta)$ على أنها الشفرة الخطية الدورية على الحقل $GF(2^r)$ حيث كثيرة حدودها المولّدة هي :

$$g(x) = (\beta^{m+1} + x)(\beta^{m+1} + x) \cdots (\beta^{m+\delta-1} + x)$$

وحيث m عدد صحيح و β عنصر بدائي في الحقل $GF(2^r)$. على سبيل المثال، الشفرة المنشأة في المثال (**٦,١,٥**) هي الشفرة $RS(8,3)$ والشفرة المنشأة في المثال (**٦,١,٧**) هي الشفرة $RS(16,5)$.

مبرهنة (٦,٢,٥)

إذا كانت C هي الشفرة $RS(2^r, \delta)$ فإن :

(أ) $n = 2^r - 1$.

(ب) $k = 2^r - \delta$.

(ج) $d = \delta$.

(د) $|C| = 2^{rk}$.

البرهان

الفقرة (أ) نحصل عليها بتطبيق المبرهنة (**٦,١,١**) والفقرتان (ب) و (د) نحصل عليهما من النتيجة (**٦,١,٤**) (لاحظ أن بُعد الشفرة الخطية على الحقل $GF(2^r)$

يساوي k وعدد كلماتها يساوي 2^{rk} وهذا يتفق مع حقيقة أن الشفرة الثنائية الخطية، أي الشفرة الخطية على الحقل $GF(2)$ لها بُعد يساوي k وعدد كلماتها يساوي 2^k).
وبرهان الفقرة (ج) نحصل عليه بتطبيق المبرهنة (٦,٢,٤) لنرى أن $d \geq \delta$ وتطبيق المبرهنة (٣,١,٧) لنرى أن $d \leq \delta$. ■

ملحوظة

بما أن $d = n - k + 1$ فنرى أن شفرات ريد وسولومن هي شفرات MDS (انظر المبرهنة (٣,١,٨)).

قبل تقديم مثال آخر ننوه إلى إمكانية النظر إلى أي شفرة C من النوع $RS(2^r, \delta)$ على أنها شفرة ثنائية؛ وذلك باستبدال كل إحداثي من إحداثيات كلمة الشفرة بكلمة ثنائية طولها r من جدول $GF(2^r)$. طول هذه الشفرة يساوي $r(2^r - 1)$ وأما طول الشفرة الثنائية التي هي شفرة على حقل جزئي وشفرة جزئية فهو $2^r - 1$. نستخدم الرمز $\hat{c}$ للتمثيل الثنائي لكلمة الشفرة $c \epsilon C$ والرمز $\hat{C}$ للشفرة الثنائية التي نحصل عليها من الشفرة C بالطريقة الموضحة في هذه الفقرة. سنرى لاحقاً (انظر المبرهنة (٧,١,١٥)) أهمية هذا التمثيل للشفرة $\hat{C}$ خاصة عند التصويب المفاجئ للأخطاء.

مثال (٦,٢,٦)

لنفرض أن $GF(2^2)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^2$ ولتكن C هي الشفرة $RS(4,2)$ حيث $g(x) = \beta + x$. استناداً إلى المبرهنة (٦,٢,٥) نرى أن طول C هو $n = 3$ وبُعدها هو $k = 2$ ومسافتها هي $d = 2$ وعدد كلماتها هو $|C| = 16$.
واستناداً إلى النتيجة (٦,١,٤) نرى أن مصفوفة مولّدة للشفرة C هي:

$$G = \begin{bmatrix} \beta & 1 & 0 \\ 0 & \beta & 1 \end{bmatrix}$$

باستخدام جدول $GF(2^2)$ نرى أن $0,1,\beta,\beta^2$ تقابل المتجهات 00,10,01,11 على التوالي. الجدول التالي يُبيّن جميع الرسائل u (عددها 16) وتمثيلها الثنائي $\hat{u}$ وكلمات C المقابلة $c = uG$ وتمثيلها الثنائي :

$\hat{u}$	u	$c = uG$	$\hat{c}$	$\hat{u}$	u	$c = uG$	$\hat{u}$
0000	00	000	000000	0001	0β	$0\beta^2\beta$	001101
1000	10	$\beta 10$	011000	1001	1β	$\beta\beta\beta$	010101
0100	$\beta 0$	$\beta^2\beta 0$	110100	0101	$\beta\beta$	$\beta^2 1\beta$	111001
1100	$\beta^2 0$	$1\beta^2 0$	101100	1101	$\beta^2\beta$	10β	100001
0010	01	$0\beta 1$	000110	0011	$0\beta^2$	$01\beta^2$	001011
1010	11	$\beta\beta^2 1$	011110	1011	$1\beta^2$	$\beta 0\beta^2$	010011
0110	$\beta 1$	$\beta^2 01$	110010	0111	$\beta\beta^2$	$\beta^2\beta^2\beta^2$	111111
1110	$\beta^2 1$	111	101010	1111	$\beta^2\beta^2$	$1\beta\beta^2$	100111

▲

تمارين

(٦,٢,٧) لتكن C هي الشفرة $RS(4,3)$ حيث كثيرة حدودها المولّدة هي $g(x) = (1 + x)(\beta + x)$.

(أ) جد كلاً من n و k و d و $|C|$ لهذه الشفرة.

(ب) استخدم النتيجة **(٦,١,٤)** لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) جد جميع كلمات الشفرة C والتمثيل الثنائي المقابل لهذه الكلمات في الشفرة $\hat{C}$ والرسائل المقابلة (شفّر هذه الرسائل مُستخدماً G التي وجدتها في الفقرة (ب)).

(٦,٢,٨) لنفرض أن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$.

ولتكن C هي الشفرة $RS(8,5)$ حيث $g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x)$ هي كثيرة حدودها المولّدة.

(أ) جد كلاً من n و k و d و $|C|$ لهذه الشفرة.

(ب) استخدم النتيجة **(٦,١,٤)** لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) شفّر كلاً من الرسائل التالية مُستخدماً G إلى كلمة شفرة في الشفرة C ومن ثم إلى كلمة شفرة في الشفرة $\hat{C}$:

(i) $10\beta^2$ (ii) 111 (iii) $\beta^2\beta^4\beta^6$.

(**٦,٢,٩**) استخدم الحقول المنشأة في التمرين (**٥,١,١٥**) لإيجاد كثيرات حدود مولّدة للشفرات $RS(2^r,\delta)$ لكل من قيم r و δ و m التالية:

(أ) $r = 2$ ، $\delta = 3$ ، $m = 2$

(ب) $r = 3$ ، $\delta = 3$ ، $m = 2$

(ج) $r = 3$ ، $\delta = 5$ ، $m = 0$

(د) $r = 4$ ، $\delta = 5$ ، $m = 0$

(هـ) $r = 5$ ، $\delta = 7$ ، $m = 0$.

(**٦,٢,١٠**) جد كل شفرة من شفرات التمرين (**٦,٢,٩**) مُبيّناً القيم n و k و d و $|C|$.

نرى استناداً إلى المبرهنة (**٦,٢,٥**) أن طول الشفرة C من النوع $RS(2^r,\delta)$ هو $n = 2^r - 1$. ولكننا أحياناً نحتاج إلى شفرات طولها مختلف عن $2^r - 1$ ويمكن إنشاء مثل هذه الشفرات بسهولة من الشفرة $RS(2^r,\delta)$ على النحو التالي:

لكل عدد صحيح s حيث $1 \le s \le 2^r - \delta$ ولكل شفرة C من النوع $RS(2^r,\delta)$ تكوّن **الشفرة المقصورة (Shortened code)** بأخذ جميع كلمات الشفرة C التي تكون إحداثياتها الأخيرة (عددها يساوي s) أصفاراً ومن ثم نحذف هذه الأصفار من الكلمات.

مثال (٦,٢,١١)

إذا كانت C هي الشفرة $RS(4,2)$ المبينة في المثال (**٦,٢,٦**) فنرى أن الشفرة المقصورة $C(1)$ ($s = 1$) هي الشفرة المكوّنة من كلمات C التي إحداثيها الأخير 0 ، أي من كلمات الشفرة: $000, \beta 10, \beta^2\beta 0, 1\beta^2 0$. وبهذا نرى أن:

$C(1) = \{00, \beta 1, \beta^2\beta, 1\beta^2\}$. ▲

ومن الممكن استخدام التمثيل بكثيرات الحدود للشفرة C من النوع $RS(2^r,\delta)$ لإنشاء الشفرة المقصورة $C(s)$ المكوّنة من كثيرات حدود C التي درجاتها أصغر من $n-s=2^r-1-s$.

فإذا كانت $g(x)$ هي كثيرة الحدود المولّدة للشفرة C فنرى أن $C(s)$ هي مجموعة كثيرات الحدود $c(x)=a(x)g(x)$ حيث $deg(a(x))<k-s=2^r-\delta-s$ ؛ (لأن $deg(g(x))=\delta$). وبهذا نجد أن مصفوفة مولّدة $G(s)$ للشفرة $C(s)$ هي :

$$G(s)=\begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-s-1}g(x) \end{bmatrix}.$$

وبمقارنة هذه المصفوفة مع المصفوفة المولّدة G للشفرة C المبينة في النتيجة (**٦,١,٤**) نجد أن $G(s)$ تتكون من أول $k-s$ صفاً من صفوف G بعد حذف الصفوف (عددها s) الأخيرة من G. وبهذا، إذا كانت الشفرة C من النوع $RS(2^r,\delta)$ لها طول n وبُعد k ومسافة d فمن الواضح أن طول الشفرة $C(s)$ يساوي $n(s)=n-s=2^r-1-s$ وبُعدها $k(s)=k-s=2^r-\delta-r$.

لإيجاد المسافة $d(s)$ للشفرة $C(s)$ لاحظ أولاً أنه إذا كانت $c_1,c_2\epsilon C(s)$ فإن المسافة بينهما تساوي المسافة بين كلمتي الشفرة C المقابلتان لهما $c_100\cdots0$ و $c_200\cdots0$. ولذا فإن $d(C(s))\geq d(C)=\delta$. أيضاً استناداً إلى المبرهنة (**٣,١,٧**) نعلم أن:

$$\begin{aligned} d(s) &\leq n(s)-k(s)+1 \\ &= 2^r-1-s(2^r-\delta-s)+1 \\ &= \delta \end{aligned}$$

إذن، $d(s)=\delta$. وأخيراً، استناداً إلى المبرهنة (**٣,١,٨**) نرى أن $C(s)$ شفرة MDS ونكون قد برهنا النتيجة التالية:

مبرهنة (٦,٢,١٢)

لتكن C شفرة من النوع $RS(2^r,\delta)$ ولتكن $C(s)$ هي الشفرة المقصورة للشفرة من النوع $RS(2^r,\delta)$ ومن الطول $n(s)$ والبُعد $k(s)$ ومسافتها $d(s)$. حينئذ:

$$n(s) = 2^r - 1 - s$$
$$k(s) = 2^r - \delta - s$$
$$d(s) = \delta$$

وكذلك، $C(s)$ شفرة MDS.

ملحوظة

من الممكن الحصول على شفرات مقصورة أخرى للشفرة $RS(2^r,\delta)$ بحذف أي s من إحداثيات كلمات الشفرة عوضاً عن حذف عدد s من الإحداثيات الأخيرة. وبما أن $RS(2^r,\delta)$ هي شفرة MDS فنرى أن أي شفرة مقصورة للشفرة $RS(2^r,\delta)$ تحقق الخصائص المبينة في المبرهنة (**٦,٢,١٢**).

مثال (٦,٢,١٣)

أنشأنا في المثال (**٦,١,٥**) الشفرة C من النوع $RS(2^3,3)$ حيث كثيرة حدودها المولّدة هي $g(x) = \beta^3 + \beta^4 x + x^2$. وبهذا نرى أن المصفوفة المولّدة للشفرة المقصورة $C(s)$ هي:

$$G(2) \leftrightarrow \begin{bmatrix} \beta^3 & \beta^4 & 1 & 0 & 0 \\ 0 & \beta^3 & \beta^4 & 1 & 0 \\ 0 & 0 & \beta^3 & \beta^4 & 1 \end{bmatrix}$$

وأن $n(2) = 5$ ، $k(2) = 3$ ، $d(2) = 3$. لاحظ أن $G(2)$ تم إنشاؤها بحذف آخر صفين ($s = 2$) من المصفوفة المولّدة G المبينة في المثال (**٦,١,٥**). ▲

(٦,٣) فك تشفير شفرات ريد وسولومن

Decoding Reed- Solomon Codes

بما أن إحداثيات كلمات الشفرة $RS(2^r,\delta)$ هي عناصر في الحقل $GF(2^r)$ فنرى أن تصويب الأخطاء في الكلمات المرسلة يحتاج علاوة على تحديد موقع الخطأ إلى معرفة

قيمة هذا الخطأ. ولهذا الغرض نُعرّف **مواقع الخطأ** (**Error Locations**) في الكلمة المستقبلة على أنها الإحداثيات التي يكون فيها نمط الخطأ لا يساوي صفراً. نقوم بتعيين عدد ليدل على موقع الخطأ فعند وقوع خطأ في الإحداثي j من الكلمة المستقبلة فيكون β^j هو **عدد موقع الخطأ** (**Error Location Number**).

(نستخدم الأعداد $0,1,2,\cdots,n-1$ لترقيم الإحداثيات كما فعلنا لشفرات BCH التي تصوّب خطأين). على سبيل المثال، تجد لنا الخطوتان (٤) و (٦) من الخوارزمية (**٥,٥,٤**) عدد موقع الخطأ لنمط الخطأ عند استخدامنا شفرة BCH التي تصوّب خطأين. **قيمة الخطأ** (**Error Magnitude**) لموقع الخطأ i هي العنصر في الحقل $GF(2^r)$ الذي يظهر في الإحداثي i من نمط خطأ. بما أن الشفرة BCH المقدمة في الفصل الخامس هي شفرة على الحقل $GF(2)$، فنرى أن جميع قيم الخطأ تساوي 1 (العنصر غير الصفري الوحيد في الحقل $GF(2)$) وبهذا فهي تتحدد تماماً بمعرفة مواقع الأخطاء. ولكن الوضع مختلف في الشفرات المعرّفة على الحقل $GF(2^r)$ حيث $r \geq 2$ ومن ثم نحتاج لفك تشفير شفرات ريد وسولومن إلى إيجاد مواقع الأخطاء وقيم الأخطاء التي تقابل هذه المواقع.

مثال (٦,٣,١)

لنفرض أن $RS(8,3)$ هي الشفرة المبينة في المثال (**٦,١,٥**). إذا كانت $c = \beta^3\beta^4\beta^0000$ هي الكلمة المرسلة و $w = \beta^3\beta^4\beta^5000$ هي الكلمة المستقبلة فنرى أن نمط الخطأ هو:

$$e = c + w = 00\beta^4 0000$$

بما أن β^4 هو العنصر غير الصفري في نمط الخطأ e وهو الإحداثي 2 فنجد أن عدد موقع الخطأ هو β^2 وأما قيمة الخطأ المقابلة فهي β^4. ▲

نقدم الآن خوارزمية لفك تشفير الشفرة $RS(2^r,\delta)$ (ومن ثم الشفرة المقابلة BCH والتي هي شفرة على حقل جزئي وشفرة جزئية). لهذا الغرض، نفرض أن:

$$g(x) = (\beta^{m+1} + x)(\beta^{m+2} + x) \cdots (\beta^{m+\delta-1} + x)$$

هي كثيرة الحدود المولّدة حيث β عنصر بدائي في الحقل $GF(2^r)$. ولنفرض أن $t = \lfloor \delta - 1/2 \rfloor$ (كما في العادة) ولنفرض أن $a_1, \cdots, a_e$ هي أعداد مواقع الأخطاء وأن $b_1, \cdots, b_e$ هي قيم الأخطاء المقابلة لهذه الأعداد حيث $e \leq t$ (في المثال (**٦,٣,١**) لدينا $t = 1$ وبما أنه وقع خطأ واحد في الموقع الثاني، نرى أن $a_1 = \beta^2$ وأن $b_1 = \beta^4$). إذا كان $e < t$ فيكون من المناسب جعل $a_i = 0$ لكل $e + 1 \leq i \leq t$ على الرغم من عدم وجود مواقع لهذه الأخطاء. نقوم الآن بحساب التناذرات $s_{m+1}, \cdots, s_{m+\delta-1}$ (عددها $\delta - 1$) وهي معرّفة على النحو التالي: $s_j = w(\beta^j)$ حيث $m + 1 \leq j \leq m + \delta - 1$. (لاحظ أن هذا هو التعريف نفسه للتناذرين s_1 و s_3 المستخدمين في الشفرة BCH). لكل $m + 1 \leq j \leq m + \delta - 1$ نرى أن β^j جذر لكثيرة الحدود المولّدة $g(x)$ ومن ثم فهو جذر لجميع كلمات الشفرة ويكون:

$$s_j = w(\beta^j) = c(\beta^j) + e(\beta^j) = e(\beta^j) = \sum_{i=1}^{t} b_i a_i^j \qquad (٦,١)$$

لاحظ أن (**٦,١**) نظام معادلات عدد معادلاته يساوي $\delta - 1$. إذن، مسألة فك التشفير تؤول إلى إيجاد طريقة فعّالة لحل نظام جزئي من نظام المعادلات (**٦,١**) عدد معادلاته $2e$ وعدد مجاهيله $2e$ وهي $a_1, \cdots, a_e, b_1, \cdots, b_e$. (لاحظ أن $2e \leq 2t \leq \delta - 1$). المشكلة الأساسية تكمن في أن هذه المعادلات غير خطية ومع ذلك سنبيّن الآن كيفية إيجاد كثيرة حدود جذورها $a_1, \cdots, a_e$ بأسلوب مماثل للخطوة (٦) من الخوارزمية (**٥,٥,٤**) التي استخدمت لفك تشفير الشفرة BCH التي تصوّب خطأين.

لنفرض إذن أن $A = \{a_1, \cdots, a_e\}$. نُعرّف **كثيرة حدود موقع خطأ** (**Error Location Polynomial**) $\sigma_A(x)$ على أنها كثيرة الحدود ذات الجذور $a_1, \cdots, a_e$. أي أن:

$$\sigma_A(x) = (a_1 + x)(a_2 + x) \cdots (a_e + x) \tag{٦,٢}$$

لنفرض الآن أن σ_j هو معامل x^j في كثيرة الحدود $\sigma_A(x)$. حينئذ، بعد ضرب عوامل $\sigma_A(x)$ نرى أن:

$$\sigma_A(x) = \sigma_0 + \sigma_1 x + \cdots + \sigma_{e-1} x^{e-1} + x^e \tag{٦,٣}$$

الآن، بضرب طرفي المعادلة بالمقدار $b_i a_i^j$ لكل $1 \le i \le e$ وتعويض $x = a_i$ وأخذ المجموع من $i = 1$ إلى $i = t$ واستخدام المعادلة (**٦,٢**) نرى أن $\sigma_A(a_i) = 0$ ومن ثم نحصل على:

$$\begin{aligned} 0 &= \left(\sum_{i=1}^{t} b_i a_i^j\right)\sigma_0 + \left(\sum_{i=1}^{t} b_i a_i^j\right)\sigma_1 + \cdots + \left(\sum_{i=1}^{t} b_i a_i^{j+e}\right) \\ &= s_j \sigma_0 + s_{j+1}\sigma_1 + \cdots + s_{j+e} \end{aligned} \tag{٦,٤}$$

أي أن:

$$s_{j+e} = s_j \sigma_0 + s_{j+1}\sigma_1 + \cdots + \sigma_{e-1} s_{j+e-1} \tag{٦,٥}$$

وبما أن القيم $s_{m+1}, s_{m+2}, \cdots, s_{m+2e}$ معلومة فيكون باستطاعتنا تعويض القيم $j = m+1, \cdots, m+e$ لنحصل على e من المعادلات الخطية في المجاهيل $\sigma_0, \cdots, \sigma_{e-1}$ التي يمكن كتابتها على شكل المعادلة المصفوفية التالية (حيث الصف i يقابل المعادلة (**٦,٥**) عندما يكون $j = m + i$):

$$\begin{bmatrix} s_{m+1} & s_{m+2} & \cdots & s_{m+e} \\ s_{m+2} & s_{m+3} & \cdots & s_{m+e+1} \\ \vdots & \vdots & & \vdots \\ s_{m+e} & s_{m+e+1} & \cdots & s_{m+2e-1} \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \sigma_{e-1} \end{bmatrix} = \begin{bmatrix} s_{m+e+1} \\ s_{m+e+1} \\ \vdots \\ s_{m+2e} \end{bmatrix} \tag{٦,٦}$$

من المهم معرفة أنه يوجد دائماً حل غير تافه لهذا النظام الخطي.

لنفرض أن M هي مصفوفة المعاملات من الدرجة e في المعادلة (٦,٦). عندئذ، رتبة M تساوي e ولرؤية ذلك لاحظ أن

$$M = \begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_e \\ \vdots & & \vdots \\ a_1^{e-1} & \cdots & a_e^{e-1} \end{bmatrix} \begin{bmatrix} b_1 a_1^{m+1} & & 0 \\ & \ddots & \\ 0 & & b_e a_e^{m+1} \end{bmatrix} \begin{bmatrix} 1 & a_1 & \cdots & a_1^{e-1} \\ \vdots & \vdots & & \vdots \\ 1 & a_e & \cdots & a_e^{e-1} \end{bmatrix}$$

وبما أن $a_1, \cdots, a_e$ عناصر مختلفة وأن $a_1, \cdots, a_e, b_1, \cdots, b_e$ جميعها عناصر غير صفرية فنرى استناداً إلى التمهيدية (٦,٢,١) أن رتبة كل من المصفوفات الثلاث تساوي e وبهذا تكون رتبة M تساوي e. بناء على ما تقدم يكون بإمكاننا حل النظام (٦,٦) لإيجاد قيم $\sigma_0, \cdots, \sigma_{e-1}$. لاحظ أنه إذا افترض فاكك التشفير ابتداءً أن $e = t$ (بالطبع إن قيمة e لا تكون معروفة مسبقاً لفاكك التشفير) فتكون M مصفوفة من الدرجة $t \times (t+1)$ رتبتها e. ويمكن رؤية ذلك بكتابة M كحاصل ضرب ثلاث مصفوفات كما في السابق واستخدام الحقيقة $a_i = 0$ لكل $e + 1 \leq i \leq t$. وبهذا تكون قيمة e معروفة الآن لدى فاكك التشفير. الآن، بما أن جذور $\sigma_A(x) = \sigma_0 + \sigma_1 x + \cdots + x^e$ هي $a_1, \cdots, a_e$ فنحصل عليها بتعويض عناصر الحقل في كثيرة الحدود $\sigma_A(x)$.

بعد إيجاد قيم $a_1, \cdots, a_e$ يتحوّل النظام (٦,١) إلى نظام معادلات خطية في المتغيرات $b_1, \cdots, b_e$ ومن ثم فباستطاعتنا حل هذا النظام بحل المعادلة المصفوفية المقابلة:

$$\begin{bmatrix} a_1^{m+1} & a_2^{m+1} & \cdots & a_e^{m+1} \\ a_1^{m+2} & a_2^{m+2} & \cdots & a_e^{m+2} \\ \vdots & \vdots & & \vdots \\ a_1^{m+e} & a_2^{m+e} & \cdots & a_e^{m+e} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_e \end{bmatrix} = \begin{bmatrix} s_{m+1} \\ s_{m+2} \\ \vdots \\ s_{m+e} \end{bmatrix} \qquad (٦,٧)$$

(مرة أخرى، نرى استناداً إلى التمهيدية (٦,٢,١) أن رتبة هذه المصفوفة تساوي e؛ وذلك لأن العناصر $a_1, \cdots, a_e$ غير صفرية وبهذا يمكن حل النظام الخطي لإيجاد $b_1, \cdots, b_e$).

مما تقدم يكون لدينا خوارزمية فك التشفير التالية لشفرات ريد وسولومن حيث نستخدم المصفوفة الموسّعة M' وهي المصفوفة M مُضافاً إليها عمود يمثل الطرف الأيمن للنظام (٦،٦). أي أن:

$$M' = \begin{bmatrix} s_{m+1} & s_{m+2} & \cdots & s_{m+e+1} \\ s_{m+2} & s_{m+3} & \cdots & s_{m+e+2} \\ \vdots & \vdots & & \vdots \\ s_{m+e} & s_{m+e+1} & \cdots & s_{m+2e} \end{bmatrix}.$$

خوارزمية (٦،٣،٢) [فك تشفير $RS(2^r, \delta)$]

لنفرض أنه تم إرسال إحدى كلمات الشفرة C من النوع $RS(2^r, \delta)$ حيث كثيرة حدودها المولّدة هي $g(x) = (\beta^{m+1} + x) \cdots (\beta^{m+\delta-1} + x)$ ولنفرض أن w هي الكلمة المستقبلة. ولنفرض أن $t = \lfloor(\delta - 1)/2\rfloor$. عندئذ، لإيجاد أقرب كلمة شفرة تنتمي إلى C إلى الكلمة w نقوم بتنفيذ الخطوات التالية:

(١) حساب $s_j = w(\beta^j)$ لكل $m + 1 \leq j \leq m + 2t$.

(٢) نضع $e = t$ ثم نجد رتبة المصفوفة الموسّعة M'.

(٣) إذا كانت e هي رتبة المصفوفة الموسّعة M' فنقوم بحل النظام الخطي (٦،٦) لإيجاد $\sigma_0, \cdots, \sigma_{e-1}$.

(٤) نجد جذور كثيرة الحدود $\sigma_A(x) = \sigma_0 + \sigma_1 x + \cdots + x^e$ فتكون هذه الجذور هي أعداد مواقع الخطأ $a_1, \cdots, a_e$.

(٥) نقوم بحل النظام الخطي (٦،٧) لإيجاد القيم $b_1, \cdots, b_e$ وهي قيم الخطأ المقابلة للقيم $a_1, \cdots, a_e$. وبهذا يتم تحديد نمط الخطأ الأرجحي.

لاحظ أننا لسنا بحاجة لوضع المصفوفة في الخطوة (٣) من الخوارزمية (٦،٣،٢) على صيغة درجية صفية؛ لأنها مصفوفة جزئية من المصفوفة في الخطوة (٢) وهذا موضّح في المثال التالي:

مثال (٦,٣,٣)

لنفرض أن:

$$g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x) = \beta^6 + \beta^5 x + \beta^5 x^2 + \beta^2 x^3 + x^4$$

كثيرة حدود مولّدة للشفرة $RS(2^3,5)$ (لاحظ أن $m=-1$ وأن $t=2$) حيث استخدمنا كثيرة الحدود x^3+x+1 لإنشاء $GF(2^3)$. ولنفرض أن $w=\beta^6\beta\beta^5\beta^2 10\beta^2$ هي الكلمة المستقبلة. سنستخدم الخوارزمية (**٦,٣,٢**) لفك تشفير w.

(١) بما أن $m=-1$ و $\delta=5$ فنقوم بحساب التناذرات الأربعة s_0,s_1,s_2,s_3 (أي حساب s_i إذا كان β^i جذراً لكثيرة الحدود $g(x)$).

$$s_0 = w(\beta^0) = \beta^6 + \beta + \beta^5 + \beta^2 + 1 + 0 + \beta^2 = 1$$
$$s_1 = w(\beta) = \beta^6 + \beta^2 + \beta^7 + \beta^5 + \beta^4 + 0 + \beta^8 = \beta^3$$
$$s_2 = w(\beta^2) = \beta^6 + \beta^3 + \beta^9 + \beta^8 + \beta^8 + 0 + \beta^{14} = \beta^3$$
$$s_3 = w(\beta^3) = \beta^6 + \beta^4 + \beta^{11} + \beta^{11} + \beta^{12} + 0 + \beta^{20} = 1$$

(٢) بوضع $e=t=2$ نرى أن المصفوفة الموسّعة M' هي:

$$M' = \begin{bmatrix} 1 & \beta^3 & \beta^3 \\ \beta^3 & \beta^3 & 1 \end{bmatrix}$$

والصيغة الدرجية لها هي:

$$\begin{bmatrix} 1 & \beta^3 & \beta^3 \\ 0 & \beta^4 & \beta^2 \end{bmatrix}$$

وبهذا نرى أن رتبتها تساوي 2.

(٣) بما أن رتبة M' تساوي 2 فتستطيع حل النظام:

$$M\begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} s_2 \\ s_3 \end{bmatrix}$$

والصيغة الدرجية الصفية للمصفوفة M هي التي حصلنا عليها في الخطوة (٢) ولذا نقوم بحل النظام:

$$\begin{bmatrix} 1 & \beta^3 \\ 0 & \beta^4 \end{bmatrix}\begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \beta^3 \\ \beta^4 \end{bmatrix}$$

وهذا يكافئ النظام :

$$\sigma_0 + \beta^3\sigma_1 = \beta^3$$
$$\beta^4\sigma_1 = \beta^2$$

من المعادلة الثانية نجد أن $\sigma_1 = \beta^5$. وبالتعويض في المعادلة الأولى نرى أن $\sigma_0 = 1$.

(٤) الآن كثيرة حدود مواقع الخطأ هي :

$$\sigma_A(x) = \sigma_0 + \sigma_1 x + x^2 = 1 + \beta^5 x + x^2$$

وبتجريب عناصر الحقل لإيجاد جذور $\sigma_A(x)$ نرى أن $\sigma_A(\beta) = 0$ و $\sigma_A(\beta^6) = 0$.
إذن، $\sigma_A(x) = 1 + \beta^5 x + x^2 = (\beta + x)(\beta^6 + x)$ ونرى أن قيمتي موقعي الخطأين هما $a_1 = \beta$ و $a_2 = \beta^6$.

(٥) نقوم الآن بحل النظام الخطي :

$$\begin{bmatrix} 1 & 1 \\ \beta & \beta^6 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} 1 \\ \beta^3 \end{bmatrix}$$

أي النظام :

$$\begin{bmatrix} 1 & 1 \\ 0 & \beta^5 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

ومنه نرى أن $\beta^5 b_2 = 1$ و $b_1 + b_2 = 1$. وعليه فإن $b_1 = \beta^6$ و $b_2 = \beta^2$. وبهذا يكون نمط الخطأ هو $e = 0\beta^6 0000\beta^2$. وكلمة الشفرة هي :

$c = w + e = \beta^6\beta^5\beta^5\beta^2 100$. ▲

مثال (٦,٣,٤)

لتكن:
$$g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x)(\beta^4+x)(\beta^5+x)$$
$$= 1 + \beta^4 x + \beta^2 x^2 + \beta x^3 + \beta^{12} x^4 + \beta^9 x^5 + x^6$$

هي كثيرة الحدود المولّدة للشفرة $RS(2^4, 7)$ ($m = -1$ ، $t = 3$) حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (الجدول (**٥,١**)). ولنفرض أن الكلمة المستقبلة هي :

$$w(x) = 1 + \beta^4 x + \beta x^3 + \beta^9 x^5 + x^6.$$

عندئذ،

(١)

$$s_0 = w(\beta^0) = 1 + \beta^4 + \beta + \beta^9 + 1 = \beta^7$$
$$s_1 = w(\beta) = 1 + \beta^5 + \beta^4 + \beta^{14} + \beta^6 = 1$$
$$s_2 = w(\beta^2) = 1 + \beta^6 + \beta^7 + \beta^{19} + \beta^{12} = \beta^9$$
$$s_3 = w(\beta^3) = 1 + \beta^7 + \beta^{10} + \beta^{24} + \beta^{18} = \beta^{12}$$
$$s_4 = w(\beta^4) = 1 + \beta^8 + \beta^{13} + \beta^{29} + \beta^{24} = \beta^9$$
$$s_5 = w(\beta^5) = 1 + \beta^9 + \beta^{16} + \beta^{34} + \beta^{30} = \beta^7$$

(٢)

$$M' = \begin{bmatrix} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 1 & \beta^9 & \beta^{12} & \beta^9 \\ \beta^9 & \beta^{12} & \beta^9 & \beta^7 \end{bmatrix} \leftrightarrow \begin{bmatrix} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 0 & \beta^{12} & \beta^7 & \beta^6 \\ 0 & \beta^7 & \beta^2 & \beta \end{bmatrix}$$
$$\leftrightarrow \begin{bmatrix} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 0 & \beta^{12} & \beta^7 & \beta^6 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

ونرى أن رتبة M هي 2 وعليه يكون وزن نمط الخطأ هو $e = 2$.

(٣) بما أن $e = 2$ فنرى أن النظام الخطي (٦,٧) هو:

$$\begin{bmatrix} \beta^7 & 1 \\ 1 & \beta^9 \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \beta^9 \\ \beta^{12} \end{bmatrix}$$

والنظام المختزل المقابل له هو:

$$\begin{bmatrix} \beta^7 & 1 \\ 0 & \beta^{12} \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \beta^9 \\ \beta^7 \end{bmatrix}$$

عندئذ، نحصل على النظام:

$$\beta^{12}\sigma_1 + \beta^7 = 0$$
$$\beta^7\sigma_0 + \sigma_1 + \beta^9 = 0$$

وبحل هذا النظام نجد أن $\sigma_1 = \beta^{10}$ و $\sigma_0 = \beta^6$.

(٤) $\sigma_A(x) = \beta^6 + \beta^{10}x + x^2 = (\beta^2 + x)(\beta^4 + x)$. ونرى أن $a_1 = \beta^2$ و $a_2 = \beta^4$.

$$\begin{bmatrix} 1 & 1 \\ \beta^2 & \beta^4 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} \beta^7 \\ 1 \end{bmatrix} \quad (٥)$$

وباختزال هذا النظام نجد أن:

$$\begin{bmatrix} 1 & 1 \\ 0 & \beta^{10} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} \beta^7 \\ \beta^7 \end{bmatrix}$$

وبحل هذا النظام نجد أن $b_1 = \beta^2$ و $b_2 = \beta^{12}$. وبهذا يكون نمط الخطأ المرجح هو:

$$e = 00\beta^2 0\beta^{12} 0 \cdots 0$$

وكلمة الشفرة المرجحة هي:

$$.c = w + e = 1\beta^4\beta^2\beta\beta^{12}\beta^9 100 \cdots 0 \quad ▲$$

لاحظ أن خوارزمية فك التشفير (**٦,٣,٢**) لا تعتمد على البنية الدورية للشفرة ولهذا فيمكن استخدامها لشفرة $RS(2^r, \delta)$ المقصورة من الطول n.

تمارين

(**٦,٣,٥**) لتكن C هي الشفرة $RS(2^4, \delta)$ وكثيرة حدودها المولّدة هي:

$$g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)(\beta^5 + x)$$

حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**)). فُك تشفير الكلمات المستقبلة التالية التي تم تشفيرها بواسطة الشفرة C:

(أ) $.0\beta^3\beta\beta^5\beta^3\beta^2\beta^6\beta^{10}\beta 000000$

(ب) $.0\beta^4\beta^2\beta 0010\beta\beta^5\beta^3\beta^2 0\beta^{10}\beta$

(ج) $.\beta 0\beta^7 0\beta^{12}\beta^3\beta^3 10000000$

(**٦,٣,٦**) لتكن C هي الشفرة $RS(2^4, \delta)$ وكثيرة حدودها المولّدة هي:

$$g(x) = (\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)$$

حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**) ولاحظ أن $m = 0$ في هذه الحالة). فُك تشفير الكلمات المستقبلة التالية إذا علمت أنها شُفّرت بواسطة الشفرة C:

(أ) $.001\beta^8 00\beta^5 00000000$

(ب) $.0\beta^{10}0\beta^6\beta^{13}0\beta^8\beta^{11}\beta^3\beta^5 00000$

(ج) $.\beta^4 0100\beta^2\beta^5\beta^{12}\beta^{14}000000$

(**٦,٣,٧**) لتكن C هي الشفرة $RS(2^4,5)$ المقدمة في التمرين (**٦,٣,٦**) ولتكن $C(4)$ هي الشفرة المقصورة من الطول $n = 11$ والبُعد $k = 7$. فُك تشفير كل من الكلمات المستقبلة التالية المشفّرة باستخدام C :

(أ) $.001\beta^8 00\beta^5 0000$

(ب) $.0\beta^{10}0\beta^6\beta^{13}0\beta^8\beta^{11}\beta^3\beta^5 0$

(ج) $.\beta^4 0100\beta^2\beta^5\beta^{12}\beta^{14}00$

(**٦,٣,٨**) لتكن C هي الشفرة $RS(2^4,9)$ وكثيرة حدودها المولّدة هي :

$$g(x) = (1 + x)(\beta + x) \cdots (\beta^7 + x)$$

حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**)). جد نمط الخطأ الأرجح للكلمات المستقبلة التي شُفّرت بواسطة الشفرة C والتي لها التناذرات التالية :

(أ) $.s_0 = \beta^2, s_1 = \beta^3, s_2 = \beta^4, s_3 = \beta^5, s_4 = \beta^6, s_5 = \beta^7, s_6 = \beta^8, s_7 = \beta^9$

(ب) $.s_0 = \beta^9, s_1 = \beta^{13}, s_2 = \beta^7, s_3 = \beta^4, s_4 = \beta^{12}, s_5 = \beta^4, s_6 = \beta^8, s_7 = \beta^2$

(ج) $.s_0 = 1, s_1 = 1, s_2 = 1, s_3 = 1, s_4 = 1, s_5 = 1, s_6 = 1, s_7 = 1$

(د) $.s_0 = \beta^{10}, s_1 = \beta^3, s_2 = \beta^{13}, s_3 = \beta^3, s_4 = \beta^{12}, s_5 = \beta^5, s_6 = \beta^{13}, s_7 = \beta^3$

(هـ) $.s_0 = \beta^{12}, s_1 = \beta^8, s_2 = 0, s_3 = \beta^7, s_4 = \beta^{13}, s_5 = \beta^4, s_6 = \beta^{13}, s_7 = 1$

(و) $.s_0 = \beta^2, s_1 = 0, s_2 = 0, s_3 = \beta^2, s_4 = 0, s_5 = 0, s_6 = \beta^2, s_7 = 0$

(٦,٤) طريقة التحويل لإنشاء شفرات ريد وسولومن
Transform Approach to Reed-Solomon Codes

تعتمد طريقة التحويل لإنشاء وفك تشفير شفرات ريد وسولومن على إمكانية تمثيل متجهات K^n كدوال من مجموعة S إلى الحقل $F = GF(2^r)$ عوضاً عن تمثيلها كمعاملات كثيرات حدود. ندرس الآن تفاصيل هذه الطريقة ونثبت أنها تُزودنا بمصفوفة مولّدة مختلفة لشفرات ريد وسولومن.

مثال (٦,٤,١)

لنفرض أن $S = GF(2^3)$ هو الحقل المنشأ باستخدام $1 + x + x^3$ والعنصر البدائي β.

ولنفرض أن $f: S \to \{0,1\}$ هي الدالة المعرّفة على النحو التالي:

$$f(0) = 0, f(1) = 0, f(\beta) = f(\beta^2) = f(\beta^4) = 1, f(\beta^6) = f(\beta^3) = f(\beta^5) = 0$$

عندئذ، يمكن تمثيل $f(x)$ بالمتجه:

$$v_f = \big(f(0), f(1), f(\beta), \cdots, f(\beta^6)\big) = (0,0,1,1,0,1,0,0).$$ ▲

مثال (٦,٤,٢)

لنفرض أن $S = GF(2^3)$ ولنفرض أن الدالة $g: S \to S$ معرّفة على النحو التالي:

$$v_g = \big(g(0), g(1), g(\beta), \cdots, g(\beta^6)\big) = (\beta^4, 0,1, \beta^2, 1, \beta, 0,0)$$

لاحظ أنه من الممكن تمثيل $g(x)$ بكثيرة الحدود:

$$g(x) = \beta^4 + \beta^2 x + \beta^3 x^2 + x^3.$$ ▲

تُمثل كثيرتا الحدود $p(x)$ و $q(x)$ الدالة نفسها من S إلى $GF(2^r)$ حيث $S \subseteq GF(2^r)$ إذا وفقط إذا كان $p(\alpha) = q(\alpha)$ لكل $\epsilon \alpha S$.

لنفرض أن V مجموعة جميع كثيرات الحدود من الدرجة التي لا تزيد عن $k - 1$ والتي معاملاتها عناصر من الحقل $GF(2^r)$ (أو مجموعة المتجهات التي تمثل كثيرات الحدود هذه كدوال من $S \subseteq GF(2^r)$ إلى $GF(2^r)$). المبرهنة التالية تُبيّن لنا أن V فضاء

متجهات ومجموعة كثيرات الحدود $\{1, x, x^2, \cdots, x^{k-1}\}$ أساس لهذا الفضاء. يُدعى فضاء المتجهات هذا **بالفضاء الدالي على S (Function Space on S)**.

مبرهنة (٦,٤,٣)

مجموعة جميع الدوال من S إلى $F = GF(2^r)$ الممثلة بكثيرات حدود من درجات لا تزيد عن $k-1$ هي فضاء دالي بُعده k وأساسه $\{1, x, x^2, \cdots, x^{k-1}\}$.

البرهان

من الواضح أن أي كثيرة حدود درجتها لا تزيد عن $k-1$ تنتمي إلى $\langle\{1, x, x^2, \cdots, x^{k-1}\}\rangle$.

ولذا نحتاج فقط إلى إثبات وحدانية التمثيل لكل دالة. ولهذا الغرض نفرض أن $p(x)$ و $q(x)$ متساويتان كدالتين على S. حينئذ، نرى أن $p(\alpha) - q(\alpha)$ لكل $\epsilon\alpha S$. وعليه فإن $p(\alpha) - q(\alpha) = 0$ وتكون $p(x) - q(x)$ كثيرة حدود درجتها أصغر من k وعدد جذورها n وهذا مستحيل ؛ لأن $n \geq k$. إذن، $p(x) - q(x) = 0$. أي أن $p(x) = q(x)$. ■

مثال (٦,٤,٤)

لنفرض أن $F = GF(2^r)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$ وليكن V هو الفضاء الدالي المكوّن من كثيرات الحدود التي درجتها لا تزيد عن 2. عندئذ، $\{1, x, x^2\}$ أساس للفضاء الدالي والمتجهات المقابلة لهذا الأساس هي :

$$1 \leftrightarrow (1,1,1,1,1,1,1,1)$$
$$x \leftrightarrow (0,1,\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6)$$
$$x^2 \leftrightarrow (0,1,\beta^2,\beta^4,\beta^6,\beta,\beta^3,\beta^5)$$

المتجه المقابل لكثيرة الحدود $p(x) = a_0 + a_1x + a_2x^2$ (باعتبارها دالة) هو :

$$v_p = [a_0, a_1, a_2]\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 0 & 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \end{bmatrix}. \quad \blacktriangle$$

تذكر أن شفرة MDS هي شفرة خطية من النوع (n,k,d) حيث $d = n - k + 1$.

مبرهنة (٦,٤,٥)

الفضاء الدالي على المجموعة $S \subseteq GF(2^r)$ المكوّن من كثيرات الحدود التي درجاتها لا تزيد عن $k - 1$ ومعاملاتها تنتمي إلى $GF(2^r)$ هو شفرة MDS من النوع $(n, k, n - k + 1)$ حيث $n = |S| \leq 2^r$.

البرهان

نفرض أن $S \subseteq GF(2^r)$ حيث $|S| = n$ ولنفرض أن الفضاء الدالي هو الفضاء المكوّن من جميع كثيرات الحدود $p: S \to GF(2^r)$ حيث $deg(p(x)) \leq k - 1$.

من الواضح أن طول كل من المتجهات (ومن ثم طول الشفرة) هو n وأن بعد الفضاء يساوي k حيث $k \leq n$ (استناداً إلى المبرهنة (**٦,٤,٣**)). ولحساب المسافة لاحظ أولاً أن عدد الجذور المختلفة لكثيرة حدود $p(x)$ حيث $deg(p(x)) \leq k - 1$ هو على الأكثر $k - 1$. وبهذا نرى أن المتجه المقابل لكثيرة الحدود $p(x)$ يحتوي على الأكثر $k - 1$ صفراً ويكون وزنه على الأقل $n - k + 1$. واستناداً إلى المبرهنة (**٣,١,٧**) نعلم أن $d \leq n - k + 1$ لأي شفرة خطية. إذن، $d = n - k + 1$. ■

تُسمى المجموعة الجزئية $S = \{\alpha \epsilon F: \alpha^n = 1\}$ من الحقل $F = GF(2^r)$ **جذور الوحدة من النوع n (nth Roots Of Unity)**. لاحظ أن n يقسم $2^r - 1$ (ولكن ليس من الضروري أن يكون $n = 2^r - 1$). وبهذا نرى أن n عدد فردي. لاحظ أيضاً أن S هي مجموعة جذور كثيرة الحدود $x^n + 1$ في الحقل F. نقول إن $\epsilon \beta S$ هو **جذر وحدة بدائي من النوع n (Primitive nth Root Of Unity)** في الحقل $GF(2^r)$ إذا كانت $S = \{1, \beta, \beta^2, \cdots, \beta^{n-1}\}$.

هذا المفهوم هو تعميم لمفهوم العنصر البدائي في الحقل وبهذا يتيح لنا فرصة إنشاء شفرات ريد وسولومن دورية من الطول n الذي يقسم $2^r - 1$ (ليس بالضرورة أن يكون $n = 2^r - 1$). إن جلّ ما درسناه سابقاً في هذا الفصل للشفرات من الطول

$n = 2^r - 1$ حيث β عنصر بدائي يبقى صحيحاً في الحالة التي يكون فيها β جذر وحدة بدائياً من النوع n.

مثال (٦,٤,٦)

لنفرض أن $F = GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ والعنصر البدائي β. جذور الوحدة من النوع 5 هي $\{1, \beta^3, \beta^6, \beta^9, \beta^{12}\}$ وجذور الوحدة من النوع 3 هي $\{1, \beta^5, \beta^{10}\}$. إذن، β^3 جذر وحدة بدائي من النوع 5 و β^5 جذر وحدة بدائي من النوع 3. ▲

قبل الشروع في إنشاء شفرات ريد وسولومن الدورية سنثبت أن كثيرتي حدود تقابلان الدالة نفسها على S إذا وفقط إذا كانتا متطابقتين قياس $1 + x^n$.

مبرهنة (٦,٤,٧)

لتكن $S \subseteq GF(2^r)$ مجموعة جميع جذور الوحدة من النوع n. ولتكن $p(x), q(x) \epsilon GF(2^r)$ عندئذ، $p(x)$ و $q(x)$ تمثلان الدالة نفسها $f: S \to GF(2^r)$ (أي $p(\beta^i) = q(\beta^i)$ لكل $\beta^i \epsilon S$) إذا وفقط إذا كان $p(x) \equiv q(x)(mod 1 + x^n)$.

البرهان

لنفرض أن $q(x) = h(x)(1 + x^n) + p(x)$ حيث $deg(p(x)) < n$. عندئذ، $q(\beta^i) = h(\beta^i)(1 + \beta^{in}) + p(\beta^i) = p(\beta^i)$؛ لأن β^i جذر لكثيرة الحدود $1 + x^n$.

ولبرهان العكس، نفرض أن $p(\beta^i) = q(\beta^i)$ لكل $\beta^i \epsilon S$. حينئذ يكون β^i جذراً لكثيرة الحدود $p(x) - q(x)$ ونرى أن:

$$p(x) - q(x) = h(x) \prod_{i=0}^{n-1} (x + \beta^i) = h(x)(1 + x^n). \qquad \blacksquare$$

مبرهنة (٦,٤,٨)

لتكن S مجموعة جذور الوحدة من النوع n في الحقل $GF(2^r)$. عندئذ، الفضاء الدالي على S المكوّن من جميع كثيرات الحدود التي تنتمي إلى $GF(2^r)[x]$ ودرجاتها لا تزيد عن $k - 1$ هو شفرة دورية من النوع $(n, k, n - k + 1)$ على الحقل $GF(2^r)$.

البرهان

لنفرض أن $v_p(p(1),p(\beta),\cdots,p(\beta^{n-1}))\epsilon C$. لإثبات أن C شفرة دورية يكفي أن نثبت أن $(p(\beta),p(\beta^2),\cdots,p(\beta^{n-1}))\epsilon C$. وبملاحظة أن $p(\beta x)$ كثيرة حدود درجتها لا تزيد عن $k-1$ نرى أن $p'(x)=p(\beta x)\epsilon C$. ولكن:

$.(p'(1),p'(\beta),\cdots,p'(\beta^{n-1})=(p(\beta),p(\beta^2),\cdots,p(\beta^{n-1}),p(1))$ ■

مثال (٦,٤,٩)

لنفرض أن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1+x+x^3$. ولتقابل $p(x)=\beta^4+\beta^2x+\beta^3x^2+x^3$ المتجه $(0,1,\beta^2,1,\beta,0,0)$. عندئذ، المتجه $(1,\beta^2,1,\beta,0,0,0)$ هو إزاحة لهذا المتجه ويقابل الدالة:

$.p(\beta x)=\beta^4+\beta^3x+\beta^5x^2+\beta^3x^3=(\beta^4+x)(\beta^5+x)(\beta^6+x)\beta^3$ ▲

لتكن $V(x)=V_0+V_1x+\cdots+V_{n-1}x^{n-1}$. نقول إن كثيرة الحدود $v(x)=v_0+v_1x+\cdots+v_{n-1}x^{n-1}$ هي **تحويل** (**Transform**) كثيرة الحدود $V(x)$ إذا كان $V(\beta^j)=\sum V_i\beta^{ji}=v_j$ لكل $j=0,1,\cdots,n-1$. وهذا يكافئ المعادلة المصفوفية $(V_0,V_1,\cdots,V_{n-1})A=(v_0,v_1,\cdots,v_{n-1})$ حيث $A=[a_{ij}]$ و $a_{ij}=\beta^{ij}$ و β جذر وحدة بدائي من النوع n في الحقل $GF(2^r)$. تُسمى المصفوفة A، **تحويل فوريبه المنتهي** (**Finite Fourier Transform**) أو **تحويل الحقل المنته** (**Finite Field Transform**). A مصفوفة قابلة للعكس ونرى أن:

$$(V_0,V_1,\cdots,V_{n-1})=(v_0,v_1,\cdots,v_{n-1})A^{-1}$$

أو $.V_i=\sum_{j=0}^{n-1}v_j\beta^{-ij}=v(\beta^{-i})$

بيّنا في التمهيدية (**٦,٢,١**) أن A قابلة للعكس ولكننا نُقدم الآن برهاناً آخر لذلك بإثبات أن A^{-1} تحوّل v إلى V.

مبرهنة (٦,٤,١٠)

لنفرض أن β جذر وحدة بدائي من النوع n. إذا كان $v_i = V(\beta^i)$ حيث $V(x) = V_0 + V_1 x + \cdots + V_{n-1}x^{n-1}$ فإن $V_i = v(\beta^{-i})$ حيث:
$.v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$

البرهان

$$v(\beta^{-i}) = \sum_j v_j \beta^{-ij} = \sum_j (\sum_k V_k (\beta^{kj})\, \beta^{-ij} = \sum_k V_k \sum_j \beta^{(k-i)j} = V_i$$

لأن

$$\sum_{j=0}^{n-1} \beta^{(k-i)j} = \begin{cases} n\, mod2, & k-i=0 \\ 0 \quad , & k-i \neq 0 \end{cases}$$

وبملاحظة أن $(1+x^n) = (1+x)(1+x+\cdots+n^{n-2}+x^{n-1})$ نرى أن $\beta^{k-i} \neq 1$ جذر لكثيرة الحدود $1+x+\cdots+x^{n-2}+x^{n-1}$. أيضاً n فردي ؛ لأن n يقسم $2^r - 1$. ■

إذا كان $(v_0, v_1, \cdots, v_{n-1})$ متجهاً فقد بيّنا كيفية استخدام هذا المتجه للحصول على معاملات كثيرة الحدود $V(x) = V_0 + V_1 x + \cdots + V_{n-1}x^{n-1}$. وهذا هو بالفعل ما تنجزه خوارزمية فك التشفير المقدمة في البند (**٦,٣**).

مبرهنة (٦,٤,١١)

لتكن S مجموعة جذور الوحدة من النوع n في الحقل $GF(2^r)$. عندئذ، الفضاء الدالي المكوّن من كثيرات الحدود التي درجاتها أصغر من $n - \delta + 1$ على S هو شفرة MDS دورية حيث $g(x) = (\beta + x)(\beta^2 + x)\cdots(\beta^{\delta-1} + x)$ كثيرة حدوده المولّدة و β جذر وحدة بدائي من النوع n.

البرهان

كثيرة الحدود $C(x)$ التي متجهها يقابل $c(x) = a(x)g(x)$ هي:

$$C(x) = \sum_{i=0}^{n=i} c(\beta^{n-i})x$$

وبما أن $c(\beta^{n-i}) = 0$ لكل $i = n - \delta + 1, n - \delta + 2, \cdots, n - 1$ فنرى أن معامل x^i في $C(x)$ يساوي صفراً وبهذا تكون $deg(C(x)) < n - \delta + 1$. ■

نستطيع القول الآن إن الطريقة البديلة التي قدّمناها لإنشاء شفرة $RS(2^r, \delta)$ حيث $n = 2^r - 1$ تُزودنا بمصفوفة مولّدة مختلفة عن تلك التي حصلنا عليها في السابق (إضافة إلى نظرة مختلفة لإحداثيات المعلومات).

مثال (٦,٤,١٢)

ليكن $\epsilon\beta GF(2^3)$ عنصراً بدائياً حيث $GF(2^3)$ هو الحقل المنشأ باستخدام $1 + x + x^3$. ولنفرض أن $RS(2^3, 5)$ هي الشفرة المبينة في المثال (**٦,٢,٨**) حيث كثيرة حدودها المولّدة هي:

$$g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x) = \beta^6 + \beta^5 x + \beta^5 x^2 + \beta^2 x^3 + x^4.$$

المتجه المقابل لكثيرة الحدود $g(x)$ هو $(\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0)$. أما تحويل $g(x)$ فهو كثيرة الحدود $G(x) = \sum_{k=0}^{6} g(\beta^{7-k}) x^k$.

بما أن $(g(\beta^0), g(\beta^1), \cdots, g(\beta^6)) = (0,0,0,0,1, \beta, \beta^4)$ فنرى أن:

$$\begin{aligned} G(x) &= g(\beta^{7-1})x + g(\beta^{7-2})x + g(\beta^{7-3})x \\ &= \beta^4 x + \beta x^2 + x^3 \\ &= x(\beta^4 + \beta x + x^2) \end{aligned}$$

ومن السهل التحقق من أن $G(x)$ تمثل دالة متجهها:

$$(G(\beta^0), G(\beta^1), \cdots, G(\beta^6)) = (\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0).$$

ننظر هنا إلى الشفرة $RS(2^3, 5)$ على أنها الفضاء الدالي لمجموعة كثيرات الحدود التي درجاتها بين 1 و 3. ومن الواضح أن $\{x, x^2, x^3\}$ أساس لهذا الفضاء الدالي وأن المصفوفة المولّدة له هي:

$$\begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^1 & \beta^3 & \beta^5 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta^1 & \beta^4 \end{bmatrix}$$

إذن، $G(x) = \beta^4 x + \beta x^2 + x^3$ إذا وفقط إذا كان المتجه المقابل لها هو:

$$(\beta^4, \beta, 1)\begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^1 & \beta^3 & \beta^5 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta^1 & \beta^4 \end{bmatrix} = (\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0).$$ ▲

نُبيّن الآن كيفية استخدام هذه الطريقة لفك تشفير شفرات ريد وسولومن. تذكر أنه إذا كانت $g(x)$ كثيرة الحدود المولّدة لشفرة ريد وسولومن وكانت $w(x)$ هي الكلمة المستقبلة فإن $w(x) = c(x) + e(x)$ حيث $c(x) = a(x)g(x)$ و $e(x)$ هي كثيرة حدود الخطأ.

لنفرض أن $W(x)$، $C(x)$، $E(x)$ هي تحويلات $w(x)$، $c(x)$، $e(x)$ على التوالي. بما أن التحويل هو تطبيق خطي نجد أن:

$$\begin{aligned} W(x) &= \sum_k w(\beta^{n-k})x^k = \sum_k c(\beta^{n-k})x^k + \sum_k e(\beta^{n-k})x^k \\ &= C(x) + E(x) \end{aligned}$$

وبما أن لكثيرة الحدود $g(x)$ عدد $\delta - 1$ من الجذور المتتالية β^k حيث $k = m+1, m+2, \cdots, m+\delta-1$ نرى أن $c(\beta^k) = 0$ وأن التناذرات s_{n-k} هي $w(\beta^{n-k}) = e(\beta^{n-k}) = E_k$ لقيم k المبينة. وهذا يعني أن التناذرات تُزودنا بعدد $\delta - 1$ من معاملات تحويل $e(x)$. ويبقى علينا إيجاد المعاملات المتبقية. ولإنجاز ذلك نحتاج كثيرة حدود مواقع الخطأ.

من تعريف $\sigma(x)$ نعلم أن $\sigma(\beta^k) = 0$ إذا وفقط إذا كان $e_k \neq 0$ (تذكر أن $\sigma(\beta^k) = 0$ إذا وفقط إذا كان β^k عدد موقع خطأ وهذه بدوره يعني أن الإحداثي k من $e(x)$ لا يساوي صفراً). وبما أن $E(\beta^k) = e_k$ فنرى أن $\sigma(\beta^k)E(\beta^k) = 0$ لكل k ويكون:

$$\sigma(x)E(x) \equiv 0 (mod 1 + x^n)$$

و $\sigma(x)E(x) \equiv \sum_{i=0}^{t} \sigma_i x^i \sum_{\ell} E_\ell x^\ell \,(mod 1 + x^n)$ (لأن درجة $\sigma(x)$ هي على الأكثر $t = \lfloor (\delta - 1)/2 \rfloor$).بمقارنة معاملات x^{t+k} نرى أن:

$$0 = \sigma_t E_k + \sigma_{t-1} E_{k+1} + \sigma_{t-2} E_{k+2} + \cdots + \sigma_0 E_{k+t}.$$

نستطيع الآن استخدام معرفتنا المسبقة لعدد $\delta - 1$ من قيم E_k المتتالية (أي، التناذرات s_{n-k}) لحساب المعاملات σ_i ومن ثم استخدام ذلك لإيجاد جميع قيم E_k.

مثال (٦,٤,١٣)

لنفرض أن $\sigma(x) = \sigma_0 + \sigma_1 x + x^2$ وأن $E(x) = E_0 + E_1 x + \cdots + E_6 x^6$. عندئذ، $\sigma(x)E(x) \equiv 0 (mod 1 + x^7)$ إذا وفقط إذا كان $E_k = \sigma_1 E_{k+1} + \sigma_0 E_{k+2}$ حيث $k = 0,1, \cdots ,6$ ▲

مثال (٦,٤,١٤)

بالرجوع إلى المثال (٦,٣,٣) نفرض أن $w = (\beta^6, \beta, \beta^5, \beta^2, 1,0, \beta^2)$. بما أن $d = 5$ فنرى أن $t \leq 2$ وأن:

$$E_0 = w(\beta^0) = 1, E_6 = w(\beta) = \beta^3, E_5 = w(\beta^2) = \beta^3, E_4 = w(\beta^3) = 1$$

وأن $\sigma(x) = x^2 + \sigma_1 x + \sigma_0$. وباستخدام المثال (٦,٣,٣) لإيجاد القيم σ_0 و σ_1 نرى أن $\sigma_0 = 1$ و $\sigma_1 = \beta^5$. وبهذا يكون $E_k = \beta^5 E_{k+1} + E_{k+2}$. وبما أن $(E_0, E_6, E_5, E_4) = (1, \beta^3, \beta^3, 1)$ فنجد أن:

$$E_3 = \beta^5 E_4 + E_5 = \beta^5 + \beta^3 = \beta^2$$
$$E_2 = \beta^5 E_3 + E_4 = \beta^5 + \beta^2 + 1 = 0$$
$$E_1 = \beta^5 E_2 + E_3 = 0 + \beta^2 = \beta^2$$

ومن ذلك يكون تحويل $e(x)$ هو $E(x) = \sum E_k x^k$ حيث:

$$(E_0, E_1, \cdots, E_6) = (1, \beta^2, 0, \beta^2, 1, \beta^3, \beta^3).$$

الآن، $E(x) = 1 + \beta^2 x + \beta^2 x^3 + x^4 + \beta^3 x^5 + \beta^3 x^6$. إذن، يكون متجه نمط الخطأ الأرجح وقوعه هو $e = \left(E(\beta^0), E(\beta^1), \cdots, E(\beta^6)\right) = (0, \beta^6, 0,0,0,0, \beta^2)$. ونخلص إلى أن كلمة الشفرة هي: $c = w + e = (\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0)$.

ومن جهة أخرى، لو استخدمنا المصفوفة المولّدة المبينة في المثال (**٦,٤,١٢**) فلا نحتاج إلى إيجاد متجه الخطأ وعوضاً عن ذلك نقوم بحساب القيم $w(\beta^k)$ لكل $k = 0,1,\cdots,6$ ومن ثم جمع هذه القيم مع تحويل $e(x)$ لنجد أن:

$$
\begin{aligned}
(w_0, w_1, \cdots, w_6) &= (w(\beta^0), w(\beta^6), w(\beta^5), \cdots, w(\beta^1)) \\
&= (1, \beta, \beta, \beta^6, 1, \beta^3, \beta^3) \\
(E_0, E_1, \cdots, E_6) &= (1, \beta^2, 0, \beta^2, 1, \beta^3, \beta^3)
\end{aligned}
$$

وبهذا يكون:

$$
\begin{aligned}
(C_0, C_1, \cdots, C_6) &= (W_0, W_1, \cdots, W_6) + (E_0, E_1, \cdots, E_6) \\
&= (0, \beta^4, \beta, 1,0,0,0)
\end{aligned}
$$

إذن، $C(x) = \beta^4 x + \beta x^2 + x^3$ وتكون إحداثيات المعلومات هي $(\beta^4, \beta, 1)$. سنترك للقارئ التحقق من أن $c = (\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0)$ هو متجه $C(x)$. ▲

تمارين

(**٦,٤,١٥**) أثبت أن $(\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0)$ هو متجه $C(x) = \beta^4 x + \beta x^2 + x^3$ حيث β عنصر بدائي في الحقل $GF(2^3)$ المنشأ باستخدام $1 + x + x^3$.

(**٦,٤,١٦**) ليكن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. جد المصفوفة المولّدة لشفرة MDS من الطول 7 للفضاء الدالي المكوّن من جميع كثيرات الحدود على $S = GF(2^3)\backslash\{0\}$ حيث أساسه هو:

(أ) $\{x, x^2, x^3\}$.

(ب) $\{1, x, x^2, x^3, x^4\}$.

(ج) $\{x, x^3, x^6\}$.

(٦,٤,١٧) أثبت أن جميع الشفرات المبينة في التمرين السابق هي شفرات دورية وجد كثيرة الحدود المولّدة لكل منها.

(٦,٤,١٨) ليكن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $x^3 + x + 1$. لكل من $G(x)$ المبينة فيما يلي ، جد المتجه المقابل v_g في الفضاء الدالي.

(أ) $G(x) = x + \beta x^3$.

(ب) $G(x) = 1 + x^2 + x^4$.

(٦,٤,١٩) لنفرض أن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $x^3 + x + 1$. ولنفرض أن β عنصر بدائي. جد معاملات كثيرة الحدود $G(x)$ إذا علمت أن :

(أ) $v_g = (\beta^3, \beta, \beta^4, 0, \beta^6, \beta^5, \beta^2)$.

(ب) $v_g = (\beta^4, \beta^2, \beta, \beta^3, 0, \beta^6, 1)$.

(٦,٤,٢٠) لكل من التمارين **(٦,٣,٥)**، **(٦,٣,٦)**، **(٦,٣,٨)**، استخدم طريقة التحويل لحساب نمط الخطأ ومن ثم فك التشفير.

(٦,٥) خوارزمية بيرلكامب ومايسي

Berlekamp-Massy Algorithm

نقدم في هذا البند خوارزمية بيرلكامب ومايسي لحساب كثيرة حدود موقع الخطأ $\sigma(x)$ بمعرفة التناذرات $s_j = w(\beta^j)$ حيث $m + 1 \le j \le m + 2t$. هذه الخوارزمية أسرع من الخوارزمية التي قدّمناها في البند السابق والتي تعتمد على حل النظام الخطي **(٦,٦)**.

لنفرض أن $\sigma_R(x) = 1 + \sigma_{t-1}x + \sigma_{t-2}x^2 + \cdots + \sigma_0 x^t$. أي أن $\sigma_R(x)$ هي عكس **(reverse)** كثيرة حدود موقع الخطأ $\sigma(x)$. ولنفرض أن $s(x) = 1 + s_{m+1}x + s_{m+2}x^2 + \cdots + s_{m+2t}x^{2t}$ هي كثيرة حدود التناذرات. باستخدام خوارزمية القسمة نجد أن :

$$\sigma_R(x)s(x) = q(x)x^{2t+1} + r(x)$$

حيث $deg(r(x)) \leq 2t$. ولكن معاملات $x^{t+1}, \cdots, x^{2t}$ في كثيرة الحدود $\sigma_R(x)s(x)$ جميعها أصفار ومن ثم فإن $deg(r(x)) \leq t$.

تُزودنا النسخة (**version**) التي نُقدمها من خوارزمية بيرلكامب ومايسي بكثيرة حدود $P_{2t}(x)$ تحقق :

$$P_{2t}(x)s(x) = q_{2t}(x)x^{2t+1} + r_{2t}(x)$$

حيث $deg(P_{2t}(x)) \leq t$ و $deg(r_{2t}(x)) \leq t$ و $P_{2t}(0) = 1$ (إن وجد). وهذا كافٍ لكي يكون $P_{2t}(x) = \sigma_R(x)$. في واقع الأمر مخرج الخوارزمية هو متتالية من كثيرات الحدود $P_i(x)$ وأعداد صحيحة D_i تحقق ما يلي :

إذا كان $P_i(x)s(x) = q_i(x)x^{i+1} + r_i(x)$ حيث $deg(r_i(x)) \leq i$ فإن $deg(P_i(x)) \leq i - \lfloor D_i/2 \rfloor$ وإن $deg(r_i(x)) \leq i - \lfloor (1 + D_i)/2 \rfloor$. إضافة إلى ذلك تكون $P_i(x)$ تركيباً خطياً لكثيرة الحدود $P_{i-1}(x)$ وكثيرة حدود سابقة $P_{z_i-1}(x)$.

لنفرض أن :

$$q_i(x) = q_{i,0} + q_{i,1}x + \cdots + q_{i,2t-1-i}x^{2t-1-i}$$

وأن :

$$.P_i(x) = x^{2t-1-i}P_i(x) = P_{i,0} + P_{i,1}x + \cdots + P_{i,\ell}x^{\ell}$$

الخطوة i من الخوارزمية هي حساب $q_i(x)$ ، $P_i(x)$ ، الأعداد الصحيحة D_i ، الدلائل z_i (التي تستخدم لتحديد كثيرة الحدود $P_{z_i}(x)$ التي نحتاج إليها إضافة إلى $P_i(x)$ لتنفيذ الخطوة التالية). إن إثبات صواب الخوارزمية أمر يسير وسنطلب من القارئ إنجاز ذلك في التمرين (**٦,٥,٥**).

خوارزمية (٦،٥،١) [خوارزمية بيرلكامب ومايسي لإيجاد كثيرة حدود موقع الخطأ]

لنفرض أن w كلمة مستقبلة تم تشفيرها باستخدام كثيرة الحدود المولّدة $g(x)$ التي جذورها القوى المتتالية $\beta^{m+1},\cdots,\beta^{m+2t}$ لعنصر β. يتم فك تشفير w بتنفيذ الخطوات التالية :

(١) احسب $s_i \coloneqq w(\beta^j)$ حيث $m+1 \le j \le m+2t$.

(٢) افرض أن :

$$q_{-1}(x) \coloneqq 1 + s_{m+1}x + s_{m+2}x^2 + \cdots + s_{m+2t}x^{2t}$$
$$q_0(x) \coloneqq s_{m+1} + s_{m+2}x + \cdots + s_{m+2t}x^{2t-1}$$
$$P_{-1}(x) \coloneqq x^{2t+1}$$
$$P_0(x) \coloneqq x^{2t}$$

افرض أن $D_{-1} \coloneqq -1$ و $D_0 \coloneqq 0$ و $z_0 \coloneqq -1$.

(٣) لكل $1 \le i \le 2t$ نقوم ارتجاعياً بتعريف $q_i(x)$ ، $P_i(x)$ ، D_i ، z_i على النحو التالي :

(أ) إذا كان $q_{i-1,0} = 0$ فنضع :

$$q_i(x) \coloneqq q_{i-1}(x)/x$$
$$P_i(x) \coloneqq P_{i-1}(x)/x$$
$$D_i \coloneqq 2 + D_{i-1}$$
$$z_i \coloneqq z_{i-1}$$

(ب) إذا كان $q_{i,0} \neq 0$ فنضع :

$$q_i(x) \coloneqq (q_{i-1}(x) - \frac{q_{i-1,0}}{q_{z_i-1,0}} q_{z_i-1}(x))/x$$

وهذه يمكن قصرها لتكون درجتها على الأكثر $2t-1-i$ ومن ثم نفرض أن :

$$P_i(x) \coloneqq (P_{i-1}(x) - \frac{q_{i-1,0}}{q_{z_i-1,0}} P_{z_i-1}(x))/x$$

$$D_i \coloneqq 2 + min\{D_{i-1}, D_{z_i-1}\}$$

$$z_i := \begin{cases} i-1, & D_i \geq D_{z_i-1} \\ z_i - 1, & \text{خلاف ذلك} \end{cases}$$

إذا وقع عدد $e \leq t$ من الأخطاء أثناء عملية الإرسال فنجد أن درجة $P_{2t}(x) = \sigma_R(x)$ تساوي e وأن كثيرة حدود موقع الخطأ هي :

$$\sigma(x) = P_{2t,e} + P_{2t,e-1}x + \cdots + P_{2t,1}x^{e-1} + x^e$$

ولها عدد e من الجذور المختلفة.

لاحظ أن خطوات الخوارزمية لا تقوم بحساب كثيرات حدود الباقي $r_i(x)$ ومع هذا يكون لكثيرات الحدود $r_{2t}(x) := P_{2t}(x)q_{-1}(x)(mod x^{2t+1})$ استخدامات أخرى في عملية فك التشفير. تُسمى $r(x) := r_{2t}(x)$ أو $\rho(x) := r_{2t}(x) - P_{2t}(x)$ **كثيرة حدود حساب الخطأ (Error Evaluator Polynomial)** وذلك لإمكانية استخدامها مع $\sigma_R'(x)$ لحساب قيم الخطأ b_j إذا علمت مواقع الخطأ a_j. فيما يلي نُبيّن كيفية إيجاد صيغة لحساب b_j بدلالة (($\rho(x)$ و $\sigma_K'(n)$) أو (($r(x)$ و $\sigma_R'(x)$). نفرض أن :

$$S(x) := \sum_{i=0}^{\infty} s_{i+m+1}x^i$$

عندئذ، نرى أن :

$$S(x) = \sum_{i=0}^{\infty}\left(\sum_{j=1}^{t} b_j a_j^{i+m+1}\right)x^i = \sum_{j=1}^{t} b_j a_j^{m+1} \sum_{i=0}^{\infty} a_j^i x^i = \sum_{j=1}^{t} \frac{b_j a_j^{m+1}}{1 - a_j x}$$

وبمـــا أن $\sigma_R(x) := \prod_{k=1}^{t}(1 - a_k x)$ فنفـــرض أن $\sigma_i(x) := \sigma_R(x)/(1 - a_j x)$ لنحصل على كثيرة الحدود $\rho(x)$ التي درجتها أصغر من درجة $\sigma(x)$

$$\rho(x) := \sigma_R(x)S(x) = \sum_{j=1}^{t} b_j a_j^{m+1}\,\sigma_j(x)$$

وبهذا يكون :

$$\rho(a_k^{-1}) = \sigma_R(a_k^{-1})S(a_k^{-1}) = \sum_{j=1}^{t} b_j a_j^{m+1}\,\sigma_j(a_k^{-1})$$

ولكن $\sigma_j(a_k^{-1}) = 0$ ما لم يكن $j = k$ ومن ذلك نرى أن $\rho(a_k^{-1}) = b_k a_k^{m+1}\sigma_k(a_k^{-1})$.

وبملاحظة أن:

$$\sigma_R'(a_k^{-1}) = -a_k \prod_{j=1, j\neq k}^{t} (1 - a_j a_k^{-1}) = -a_k \sigma_k(a_k^{-1})$$

نجد أن:

$$b_k = -\frac{\rho(a_k^{-1})}{a_k^m \sigma_R'(a_k^{-1})}$$

وبما أن $\sigma_R(a_k^{-1}) = 0$ فمن الممكن اعتبار البسط $a_k r(a_k^{-1})$ عوضاً عن $\rho(a_k^{-1})$ لنحصل على:

$$.b_k = -\frac{r(a_k^{-1})}{a_k^{m-1}\sigma_R'(a_k^{-1})}$$

مثال (٦,٥,٢)

لنأخذ المثال (**٦,٣,٤**) والتناذرات $s_0 = \beta^7, s_1 = \beta^0, s_2 = \beta^9, s_3 = \beta^{12}, s_4 = \beta^9, s_5 = \beta^7$. بتنفيذ خطوات الخوارزمية (**٦,٥,١**) نحصل على:

$$q_{-1}(x) = 1 + \beta^7 x + x^2 + \beta^9 x^3 + \beta^{12} x^4 + \beta^9 x^5 + \beta^7 x^6$$
$$q_0(x) = \beta^7 + x + \beta^9 x^2 + \beta^{12} x^3 + \beta^9 x^4 + \beta^7 x^5$$
$$P_{-1}(x) = x^7$$
$$P_0(x) = x^6$$
$$D_{-1} = -1\,, D_0 = 0\,, z_0 = -1$$

نفرض الآن أن $i = 1$. وبما أن $q_{0,0} = \beta^7 \neq 0$ فنحصل من الخطوة (٣ب) على:

$$q_0(x) + \beta^7 q_{-1}(x))/x = \beta^3 + x + \beta^{13}x^2 + \beta^{14}x^3 + \beta^{14}x^4 + \beta^{14}x^5$$

وبقصرها إلى الدرجة $2t - i - 1 = 4$ نحصل على:

$$q_1(x) = \beta^3 + x + \beta^{13}x^2 + \beta^{14}x^3 + \beta^{14}x^4$$
$$P_1(x) = 1 + \beta^7 x$$
$$D_1 = 2 + min\{D_{-1}, D_0\} = 0$$

ولكون $D_0 \geq D_{-1}$ نجد أن $z_i = i - 1 = 0$. وبتبني ترميز مختصر لتمثيل كثيرات الحدود بكلماتها المقابلة نحصل على الجدول التالي :

i				q_i					p_i		D_i	z_i
	-1	β^0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0	-1	
	0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0		0	-1
	1	β^3	β^0	β^{13}	β^{14}	β^{14}	—	β^0	β^7		1	0

وبتكملة الجدول من $i = 2$ إلى $i = 2t = 6$ نحصل على الجدول :

i			q_i				—	p_i		D_i	z_i
-1	β^0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0	-1	
0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0		0	-1
1	β^3	β^0	β^{13}	β^{14}	β^{14}	—	β^0	β^7		1	0
2	β^{12}	β^7	β^6	β^{12}	—	β^0	β^8			2	1
3	β^0	β^{10}	β^9	—	β^0	β^{12}	β^1			3	2
4	0	0	—	β^0	β^{10}	β^6				4	3
5	0	—	β^0	β^{10}	β^6					6	3
6	—	β^0	β^{10}	β^6						8	3

وأخيراً نحصل على $\sigma(x)$ بقراءة $P_{2t}(x) = P_6(x)$ عكسياً لنجد :

$$\sigma(x) = \beta^6 + \beta^{10}x + x^2.$$ ▲

مثال (٣,٥,٦)

لتكن C هي الشفرة $RS(2^4, 9)$ حيث كثيرة حدودها المولّدة هي $g(x) = (1 + x)(\beta + x) \cdots (\beta^7 + x)$ والحقل $GF(2^4)$ منشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (٥,١)). لنفرض أن w هي الكلمة المستقبلة وأن تناذرات w هي :

$$s_0 = \beta^{12}, s_1 = \beta^9, s_2 = \beta^6, s_3 = \beta^3, s_4 = \beta^5, s_5 = \beta^{12}, s_6 = \beta^6, s_7 = \beta^6$$

باستخدام الخوارزمية (**٦,٥,١**) والترميز المستخدم في المثال (**٦,٥,٢**) نحصل على كثيرة حدود موقع الخطأ على النحو التالي:

i				q_i					—	p_i		D_i	z_i
-1	β^0	β^{12}	β^9	β^6	β^3	β^5	β^{12}	β^6	β^6	—	β^0	-1	
0	β^{12}	β^9	β^6	β^3	β^5	β^{12}	β^6	β^6	—	β^0		0	-1
1	0	0	0	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}		1	0
2	0	0	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}			3	0
3	0	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}				5	0
4	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}					7	0
5	0	β^8	β^5	—	β^0	β^{12}	0	0	β^{13}			2	4
6	β^8	β^5	—	β^0	β^{12}	0	0	β^{13}				4	4
7	0	—	β^0	β^{12}	β^{13}	β^{10}	β^{13}					6	4
8	—	β^0	β^{12}	β^{13}	β^{10}	β^{13}						8	4

إذن، كثيرة حدود موقع الخطأ هي:

$$\sigma(x) = \beta^{13} + \beta^{10}x + \beta^{13}x^2 + \beta^{13}x^3 + x^4.$$ ▲

ملحوظة

لاحظ أن قيمة z_i في كل من خطوات الخوارزمية (**٦,٥,١**) هي $i-1$ أو z_{i-1}. وعليه نحتاج فقط إلى تخزين q_{i-1} ، p_{i-1} ، D_{i-1} ، z_{i-1} ، $q_{z_{i-1}}$ ، $p_{z_{i-1}}$ ولا نحتاج إلى تخزين جميع القيم الأخرى التي تم حسابها سابقاً كما هو موضح في جدولي المثالين (**٦,٥,٢**) و (**٦,٥,٣**). ومن الواضح أن ذلك يوفر الكثير من الوقت عند التطبيق العملي للخوارزمية ولكن لغرض توضيح الخوارزمية يكون من المناسب وضع جميع الحسابات في جدول واحد.

تمارين

(**٦,٥,٤**) لتكن C هي الشفرة $RS(2^4,9)$ حيث $g(x) = (1+x)(\beta+x)\cdots(\beta^7+x)$ هي كثيرة حدودها المولّدة وحيث $GF(2^4)$ منشأ باستخدام كثيرة الحدود $1+x+x^4$ (انظر الجدول (**٥,١**)). استخدم الخوارزمية (**٦,٥,١**) لإيجاد كثيرة حدود موقع الخطأ للكلمات المستقبلة التي تم تشفيرها بواسطة C والتي لها التناذرات التالية :

(أ) $s_0 = \beta^2, s_1 = \beta^3, s_2 = \beta^4, s_3 = \beta^5, s_4 = \beta^6, s_5 = \beta^7, s_6 = \beta^8, s_7 = \beta^9$.

(ب) $s_0 = \beta^9, s_1 = \beta^{13}, s_2 = \beta^7, s_3 = \beta^4, s_4 = \beta^{12}, s_5 = \beta^4, s_6 = \beta^8, s_7 = \beta^2$.

(ج) $s_0 = 1, s_1 = 1, s_2 = 1, s_3 = 1, s_4 = 1, s_5 = 1, s_6 = 1, s_7 = 1$.

(د) $s_0 = \beta^{10}, s_1 = \beta^3, s_2 = \beta^{13}, s_3 = \beta^3, s_4 = \beta^{12}, s_5 = \beta^5, s_6 = \beta^{13}, s_7 = \beta^3$.

(هـ) $s_0 = \beta^{12}, s_1 = \beta^8, s_2 = 0, s_3 = \beta^7, s_4 = \beta^{13}, s_5 = \beta^4, s_6 = \beta^{13}, s_7 = 1$.

(و) $s_0 = \beta^2, s_1 = 0, s_2 = 0, s_3 = \beta^2, s_4 = 0, s_5 = 0, s_6 = \beta^2, s_7 = 0$.

(**٦,٥,٥**) **[اثبات صواب خوارزمية بيرلكامب ومايسي]**

(أ) أثبت إرجاعياً أن $deg(P_i(x)) \le i - \lfloor D_i/2 \rfloor$ (لاحظ $P_i(0) = 1$).

(ب) أثبت إرجاعياً أن $deg(R_i(x)) \le i - \lfloor (1+D_i)/2 \rfloor$ وذلك بعد إثبات أن اختيار $q_i(0)$ يجعل معامل x^i في كثيرة الحدود $P_i(x)q_{-1}(x)$ يساوي صفراً.

(ج) أثبت أن كون جميع قيم D_j مختلفة يؤدي إلى أن تكون قيمة على الأقل من قيم $j \le i, D_j$ تساوي على الأقل i واستنتج أن $D_j \ge i$ أو $D_{z_i} \ge i$.

(د) إذا كان $D_{2t} \ge 2t$ فأثبت أن $deg(P_{2t}(x)) \le t$ وأن عدد t على الأقل من معاملات $P_{2t}(x)q_{-1}(x)$ المتتالية تساوي صفراً ؛ (لأن $deg(R_{2t}(x)) \le t$). وهذا يعني أن على الأقل t من متطابقات نيوتن المتتالية يجب أن تكون متحققة.

(٦,٦) الكلمات المحوّة

Erasures

الكلمة المحوة هي خطأ حيث عدد موقع الخطأ معلوم ولكن قيمة الخطأ غير معلومة. يمكن معرفة عدد موقع الخطأ من قراءة الإشارة المستقبلة (الإحداثي المستقبل لا يشبه الصفر أو الواحد) أو من بنية الشفرة. على سبيل المثال، لنفرض أن C شفرة من النوع $RS(2^r,\delta)$ وأن $\hat{C}$ التمثيل الثنائي للشفرة C. ولتكن $\widehat{C'}$ هي الشفرة الثنائية التي نحصل عليها من C بإضافة إحداثي اختبار النوعية للتمثيل الثنائي لكل إحداثي في كل كلمة من كلمات الشفرة C.

مثال (٦,٦,١)

لنفرض أن C هي الشفرة $RS(4,2)$ المقدمة في المثال (**٦,٢,٦**). لإنشاء $\widehat{C'}$ نقوم باستبدال الإحداثيات 0، 1، β، β^2 في كلمات الشفرة C بالكلمات 000، 101، 011، 110 على التوالي (الإحداثي الثالث في هذه الكلمات هو إحداثي اختبار النوعية). إذن، كلمة الشفرة التي تنتمي إلى $\widehat{C'}$ المقابلة لكلمة الشفرة $\beta 10 \epsilon C$ هي 011101000. ▲

تمرين

(**٦,٦,٢**) لتكن C هي الشفرة $RS(4,3)$ حيث $g(x)=(1+x)(\beta+x)$ هي كثيرة حدودها المولّدة (انظر التمرين (**٦,٢,٧**)). جد جميع كلمات الشفرة $\widehat{C'}$.

لاحظ أن كلاً من إحداثيات كلمة شفرة $c \epsilon C$ حيث C هي الشفرة $RS(2^r,\delta)$ يتم تمثيلها بكلمة ثنائية من الطول $r+1$ في كلمة الشفرة المقابلة $\widehat{c'} \epsilon \widehat{C'}$ ذات الطول $(2^r-1)(r+1)$. وبما أن أي إحداثي غير صفري من إحداثيات كلمة الشفرة c يتم استبداله بكلمة ذات وزن زوجي في الشفرة $\widehat{C'}$ فنرى أن الشفرة $\widehat{C'}$ تحتوي على 2^r-1 كلمة طول كل منها $r+1$ ووزن كل منها عدد زوجي. وبهذا نرى أنه إذا كان وزن إحدى المجموعات 2^r-1 فردياً في الكلمة المستقبلة $\widehat{w'}$ فيكون قد وقع خطأ في أحد الإحداثيات $r+1$. عندئذ، يكون باستطاعتنا فك تشفير $\widehat{w'}$ على أنها الكلمة w. أي

الكلمة التي إحداثياتها في الحقل $GF(2^r)$ التي تقابل $\widehat{w'}$ إحداثياً كلمة شفرة في الشفرة C. وعليه فمعرفتنا بوقوع أخطاء في مجموعة مكوّنة من $r+1$ إحداثياً تقابل معرفتنا بعدد موقع الخطأ واحد من w وبهذا يكون هذا الخطأ كلمة ممحوّة.

مثال (٦,٦,٣)

لتكن $\widehat{C'}$ الشفرة المقدمة في المثال (**٦,٢,٦**). ولنفرض أن 000 100 011 هي الكلمة المستقبلة. عندئذ، يكون قد وقع خطأ في المجموعة الثانية المكوّنة من ثلاث إحداثيات ؛ (لأن وزن هذه المجموعة فردي) وبهذا يكون β^1 عدد موقع كلمة ممحوة. وبما أن هذا الموقع في w هو كلمة ممحوّة فنستطيع استبداله بالإحداثي 0 (لكي يسهل عملية ايجاد التناذرات) وبهذا نقوم بفك تشفير $w=\beta 00$ إلى أقرب كلمة شفرة من كلمات الشفرة C على اعتبار أن $a_1=\beta$ هو عدد موقع الخطأ. ▲

مبرهنة (٦,٦,٤)

لتكن C هي الشفرة $RS(2^r,\delta)$ المستخدمة في إرسال رسائل. ولنفرض أن w كلمة مستقبلة تحتوي على عدد ε من الكلمات المحوّة وعدد e من الأخطاء التي ليست كلمات ممحوّة. إذا كان $2e+\varepsilon \leq \delta-1$ فعندئذ، نستطيع فك تشفير w بشكل صائب.

البرهان

لنفرض أن B مجموعة مواقع الكلمات المحوّة ولنفرض أن A مجموعة مواقع الأخطاء. حينئذ، تكون $A-B$ مجموعة مواقع الأخطاء التي ليست مواقع كلمات ممحوّة. وإذا كانت :

$$\sigma_B(x)=\prod_{i\epsilon B}(\beta^i+x)$$

كثيرة حدود مواقع الكلمات المحوّة، فنجد أن :

$$\sigma_A(x)=\sigma_B(x)\sigma_{A-B}(x).$$

لإيجاد مواقع الخطأ نحتاج إلى معرفة جذور كثيرة الحدود $\sigma_{A-B}(x)$. وإذا كان بإمكاننا إزالة تأثير الكلمات الممحوّة على التناذرات فحينئذ، نستطيع توظيف الخوارزمية (٦,٣,٢) أو الخوارزمية (٦,٥,١) لإيجاد جذور $\sigma_{A-B}(x)$ (بعد تعديل التناذرات).

لمعرفة التناذرات المعدّلة نجري تعديلاً بسيطاً على الخوارزمية (٦,٣,٢) فنفرض أن $\sigma_B(x) = B_0 + B_1x + \cdots + B_{\varepsilon-1}x^{\varepsilon-1} + x^\varepsilon$ وأن:

$$.\sigma_{A-B}(x) = A_0 + A_1x + \cdots + A_{e-1}x^{e-1} + x^e$$

وبالطريقة نفسها التي استخدمناها للحصول على (٦,٤)، نقوم بضرب طرفي المعادلة $\sigma_A(x) = \sigma_B(x)\sigma_{A-B}(x)$ بالمقدار $b_ia_i^j$ حيث $m+1 \le j \le m+\delta-1$ وحيث $a_1, \cdots, a_{e+\varepsilon}$ هي أعداد مواقع الأخطاء، ثم تعويض $x = a_i$ وجمع الطرفين من $i = 1$ إلى $e+\varepsilon$ لنحصل على:

$$\begin{aligned}(B_0s_j + B_1s_{j+1} + \cdots + B_{\varepsilon-1}s_{j+\varepsilon-1} + s_{j+\varepsilon})A_0 \\ + (B_0s_{j+1} + B_1s_{j+2} + \cdots + B_{\varepsilon-1}s_{j+\varepsilon} + s_{j+\varepsilon+1})A_1 + \cdots \\ + (B_0s_{j+e} + B_1s_{j+e+1} + \cdots + s_{j+e+\varepsilon}) = 0\end{aligned} \quad (٦,٨)$$

وبهذا نجد التناذرات المعدّلة بوضع:

$$.s_j^* = B_0s_j + B_1s_{j+1} + \cdots + B_{\varepsilon-1}s_{j+\varepsilon-1} + s_{j+\varepsilon}$$

لاحظ أن s_j^* مقادير معلومة لكل $m+1 \le j \le \delta - 1 - \varepsilon$؛ لأن s_j مقادير معلومة لكل $m+1 \le j \le m+\delta-1$ وأن $B_0 + \cdots + B_{\varepsilon-1}$ مقادير معلومة. وبما أن $2e + \varepsilon \le \delta - 1$ (أي $2e \le \delta - 1 - \varepsilon$) فيكون بامكاننا حل نظام المعادلات الخطية (٦,٩) الذي نحصل عليه من (٦,٨) بصورة مشابهة تماماً لحل نظام المعادلات الخطية الذي حصلنا عليه من (٦,٦) وبذلك نحصل على المجاهيل $A_0, A_1, \cdots, A_{e-1}$.

$$\begin{bmatrix} s_{m+1}^* & s_{m+2}^* & \cdots & s_{m+e}^* \\ \vdots & \vdots & & \vdots \\ s_{m+e}^* & s_{m+e+1}^* & \cdots & s_{m+2e-1}^* \end{bmatrix} \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{e-1} \end{bmatrix} = \begin{bmatrix} s_{m+e+1}^* \\ \vdots \\ s_{m+2e}^* \end{bmatrix} \quad (٦,٩) \quad ■$$

نقوم الآن بتعديل الخوارزمية (**٦,٣,٢**) كما هو مبيّن في المبرهنة (**٦,٦,٤**) لنحصل على خوارزمية لفك تشفير شفرة ريد وسولومن التي تحتوي على كلمات محوّة.

خوارزمية (٦,٦,٥) [فك تشفير الكلمات المحوّة في الشفرة $RS(2^r,\delta)$]

لتكن C هي الشفرة $RS(2^r,\delta)$ ولتكن $c\epsilon C$ ولتكن:

$g(x)=(\beta^{m+1}+x)\cdots(\beta^{m+\delta-1}+x)$ كثيرة الحدود المولّدة التي تم ارسالها ولنفرض أن w هي الكلمة المستقبلة التي تحتوي على عدد ε من الكلمات المحوّة حيث أعداد مواقع الكلمات المحوّة هي عناصر المجموعة $B=\{a_1,\cdots,a_\varepsilon\}$. ولنفرض أن $\sigma_B(x)=(a_1+x)\cdots(a_\varepsilon+x)=B_0+B_1x+\cdots+B_{\varepsilon-1}x^{\varepsilon-1}+x^\varepsilon$ هي كثيرة حدود مواقع الكلمات المحوّة. نحصل على كثيرة حدود مواقع الخطأ $\sigma_A(x)=\sigma_B(x)\sigma_{A-B}(x)$ بإيجاد $\sigma_{A-B}(x)=A_0+A_1x+\cdots+A_{e-1}x^{e-1}+x^e$ على النحو التالي:

(١) نقوم بحساب $s_j=w(\beta^j)$ لكل $m+1\le j\le m+\delta-1$.

(٢) نقوم بحساب $s_j^*=B_0s_j+B_1s_{j+1}+\cdots+B_{\varepsilon-1}s_{j+\varepsilon-1}+s_{j+\varepsilon}$ لكل $m+1\le j\le m+\delta-1-\varepsilon$.

(٣) نجد $A_0,A_1,\cdots,A_{e-1}$ بحل النظام الخطي (**٦,٩**).

(٤) نقوم بتنفيذ الخطوتين (٤) و (٥) من الخوارزمية (**٦,٣,٢**) لفك تشفير w.

بتوظيف التناذرات المعدّلة في الخوارزمية (**٦,٦,٥**) يكون بمقدورنا تعديل الخوارزمية (**٦,٥,١**) لإيجاد كثيرة حدود الخطأ في حالة وجود كلمات محوّة.

خوارزمية (٦,٦,٦) [فك تشفير بيرلكامب ومايسي بوجود كلمات محوّة]

لنفرض أن C هي الشفرة $RS(2^r,\delta)$ ولنفرض أن:

$g(x)=(\beta^{m+1}+x)\cdots(\beta^{m+\delta-1}+x)$ هي كثيرة الحدود المولّدة ولنفرض أن w هي الكلمة المستقبلة. ولتكن $\sigma_B(x)=B_0+B_1x+\cdots+x^\varepsilon$ كثيرة حدود موقع الخطأ

للكلمة w. يتم تعديل الخوارزمية (**٦,٥,١**) لإيجاد كثيرة حدود موقع الخطأ للكلمة w على النحو التالي:

(١) نقوم بحساب $s_j = w(\beta^j)$ لكل $m + 1 \leq j \leq m + \delta - 1$.

(٢) نقوم بحساب $s_j^* = B_0 s_j + B_1 s_{j+1} + \cdots + B_{\varepsilon-1} s_{j+\varepsilon-1} + s_{j+\varepsilon}$ لكل $m + 1 \leq j \leq m + \delta - 1 - \varepsilon$.

(٣) نضع $q_{-1}(x) = 1 + s_{m+1}^* x + s_{m+1}^* x^2 + \cdots + s_{m+\delta-1-\varepsilon}^* x^{m+\delta-1-\varepsilon}$

$$q_0(x) = s_{m+1}^* + s_{m+2}^* x + \cdots + s_{m+\delta-2-\varepsilon}^* x^{m+\delta-2-\varepsilon}$$

ونعرّف $P_{-1}(x)$ ، $P_0(x)$ ، D_{-1} ، P_0 ، z_0 كما في الخطوة (٢) من الخوارزمية (**٦,٥,١**).

(٤) نكرّر الخطوة (٣) من الخوارزمية (**٦,٥,١**) لنجد $\sigma_{A-B}(x)$ مع مراعاة أن i تقع في الفترة $1 \leq i \leq \delta - 1$.

عندئذ، تكون كثيرة حدود موقع الخطأ هي $\sigma_A(x) = \sigma_B(x)\sigma_{A-B}(x)$.

ملحوظة

لإنهاء عملية فك التشفير نوظّف الخطوة (٥) من الخوارزمية (**٦,٣,٢**) ونستخدم التناذرات الأصلية لإيجاد $b_1, b_2, \cdots, b_{\varepsilon+e}$ (من الواضح أن (**٦,٧**) هو الآن نظام معادلات خطية عدد معادلاته يساوي $e + \varepsilon$).

نستخدم في الأمثلة التالية الشفرة $\widehat{C'}$ لإرسال الرسائل وبهذا يمكن التعرف على بعض الكلمات الممحوّة من بنية (تركيب) الشفرة.

مثال (٦,٦,٧)

لتكن C هي الشفرة $RS(2^4, 6)$ ولتكن $g(x) = (1 + x)(\beta + x) \cdots (\beta^4 + x)$ هي كثيرة الحدود المولّدة حيث استخدمت كثيرة الحدود $1 + x + x^4$ لإنشاء $GF(2^4)$. ولنفرض أن الشفرة $\widehat{C'}$ هي الشفرة المستخدمة لتشفير الرسائل. فُك تشفير الكلمة المستقبلة:

$$\widehat{w'} = 11101 \quad 11001 \quad 00101 \quad 00000 \quad 00110 \quad 10010 \quad 0 \cdots 0$$

الحل

عدد موقع الكلمة الممحوّة الوحيدة هنا هو β^1. ولذا فإن $\sigma_B(x) = \beta + x$.

نوظّف الآن الخوارزمية (**٦,٦,٦**) لإيجاد كثيرة حدود موقع الخطأ للكلمة :

$$w = \beta^{10}0\beta^2 0\beta^6\beta^{14}0 \cdots 0$$

حيث وضعنا القيمة 0 للإحداثي المقابل للكلمة الممحوّة (إن ذلك يسهّل علينا حساب التناذرات).

بما أن :

$$w(x) = \beta^{10} + \beta^2x^2 + \beta^6x^4 + \beta^{14}x^5$$

فنرى أن $s_4 = \beta^3, s_3 = \beta^4, s_2 = \beta^3, s_1 = 0, s_0 = \beta^5$. وبما أن $B_0 = \beta$ وأن $\mathcal{E} = 1$ فنجد من الخطوة (٢) أن $s_0^* = \beta^6$ ، $s_1^* = \beta^3$ ، $s_2^* = 0$ ، $s_3^* = \beta^{11}$. وباستخدام الطريقة المستخدمة في الخوارزمية (**٦,٥,١**) مع استخدام التناذرات المعدّلة نحصل على :

i	p_i										q_i		D_i	z_i
-1	1	β^6	β^3	0	β^{11}							1	-1	
0	β^6	β^3	0	β^{11}							1		0	-1
1	β^{10}	β^9	β^{11}							1	β^6		1	0
2	β^0	β^{11}							1	β^{12}			2	1
3	β^{10}						1	β^{14}	β^{11}				3	2
4					1	β^{11}	β^8						4	3

ونرى أن $\sigma_{A-B}(x) = \beta^8 + \beta^{11}x + x^2$. إذن ،

$$\begin{aligned}\sigma_A(x) &= \sigma_B(x)\sigma_{A-B}(x)\\ &= (\beta + x)(\beta^8 + \beta^{11}x + x^2)\\ &= (\beta + x)(\beta^3 + x)(\beta^5 + x)\end{aligned}$$

وبهذا تكون أعداد موقع الخطأ هي $a_1 = \beta$ ، $a_2 = \beta^2$ ، $a_3 = \beta^5$. لإكمال فك التشفير نجد الآن b_1 ، b_2 ، b_3 بتطبيق الخطوة (٥) من الخوارزمية (**٦,٣,٢**) والتناذرات الأصلية والصيغة (**٦,٧**) فنجد:

$$\begin{bmatrix} 1 & 1 & 1 \\ \beta & \beta^3 & \beta^5 \\ \beta^2 & \beta^6 & \beta^{10} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} \beta^5 \\ 0 \\ \beta^3 \end{bmatrix}$$

أو

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & \beta^9 & \beta^2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} \beta^5 \\ \beta^6 \\ \beta^3 \end{bmatrix}$$

وبحل هذا النظام نرى أن $b_3 = \beta^3$ ، $b_2 = 1$ ، $b_1 = \beta^{12}$ وبهذا يكون فك تشفير $w(x)$ هو:

$$\begin{aligned} c(x) &= w(x) + e(x) \\ &= (\beta^{10} + \beta^2 x^2 + \beta^6 x^4 + \beta^{14} x^5) + (\beta^{12} x + x^3 + \beta^3 x^5) \end{aligned}$$

$$c(x) \leftrightarrow \beta^{10}\beta^{12}\beta^2 1\beta^6 10 \cdots 0$$

وبالتالي ففك تشفير $\widehat{w'}$ هو:

$11101 \quad 11110 \quad 00101 \quad 10001 \quad 00110 \quad 10001 \quad 0\cdots 0$. ▲

مثال (٦,٦,٨)

إذا استخدمت الشفرة $\widehat{C'}$ المبينة في المثال (**٦,٦,٧**) لتشفير الرسائل فَفُك تشفير $\overline{f}(w) = 11101 \quad 11001 \quad 00101 \quad 00100 \quad 00110 \quad 10010 \quad 0\cdots 0$.

الحل

كثيرة حدود موقع الكلمة الممحوّة هي:

$\sigma_B(x) = (\beta + x)(\beta^3 + x) = \beta^4 + \beta^9 x + x^2$.

ولهذا نقوم بفك تشفير:

$$w = \beta^{10} 0 \beta^2 0 \beta^6 \beta^{14} 0 \cdots 0$$

إلى كـلمة شفـرة مـن كـلمات C (مـرة أخـرى وضـعنا القـيمة 0 للإحـداثي المقــابل للكلمــة المحــوّة). بمــا أن $w(x) = \beta^{10} + \beta^2 x^2 + \beta^6 x^4 + \beta^{14} x^5$ فنــرى أن $s_4 = \beta^3, s_3 = \beta^4, s_2 = \beta^3, s_1 = 0, s_0 = \beta^5$. باسـتخدام الخطـوة (٢) مـن الخوارزميـة (٦,٦,٦) نجد أن $s_0^* = \beta$ ، $s_1^* = \beta^6$ ، $s_2^* = \beta^{11}$. وبهذا نحصل على :

i		p_i				q_i			D_i	z_i
-1	1	β^1	β^6	β^{11}				1	-1	
0	β^1	β^6	β^{11}				1		0	-1
1	β^3	β^8				1	β		1	1
2	0				1	β^5			2	2
3				1	β^5				4	3

إذن، $\sigma_{A-B}(x) = \beta^5 + x$. ويكون $\sigma_A(x) = (\beta + x)(\beta^3 + x)(\beta^5 + x)$. وبالتالي نستطيع حساب قيمة الخطأ كما في المثال (٦,٦,٧). ▲

إذا كانت C هي الشفرة $RS(2^r, \delta)$ فإن مسافة الشفرة $\widehat{C'}$ هي على الأقل 2δ وبهذا فهي تصوّب جميع أنماط الخطأ الثنائية ذوات الأوزان التي لا تزيد عن $\delta - 1$. سنبيّن الآن أنه بتنفيذ الخوارزمية (٦,٦,٦) نستطيع إيجاد أقرب كلمة شفرة للكلمة المستقبلة إذا كان عدد الأخطاء الثنائية الواقعة أثناء عملية إرسال $\widehat{c'}$ لا يزيد عن $\delta - 1$. لرؤية ذلك، نفرض أن u نمط خطأ ثنائي حيث $wt(u) \leq \delta - 1$ وحيث إن u يتسبب بوقوع عدد ε من الكلمات المحوّة وعدد e من الأخطاء التي ليست كلمات محوّة. وبما أنه يجب أن يقع على الأقل خطآن في الكلمة $\widehat{w'}$ ليحدث خطأ في w وهذا الخطأ ليس كلمة محوّة فإن $2e + \varepsilon \leq \delta - 1$. بتوظيف المبرهنة (٦,٦,٤) نرى فك تشفير w صحيح (ومن ثم فك تشفير $\widehat{w'}$). أما إذا كانت نتيجة فك تشفير $\widehat{w'}$ باستخدام الخوارزمية (٦,٦,٦) هي كلمة شفرة $\hat{c}$ تبعد بمسافة أكبر من $\delta - 1$ عن $\widehat{w'}$ فإننا لا نستطيع ضمان أن $\widehat{c'}$ هي بالفعل كلمة الشفرة الأقرب إلى $\widehat{w'}$.

تمارين

(**٦,٦,٩**) لتكن C هي الشفرة $RS(2^3,5)$ ولتكن $g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x)$ حيث استخدمت كثيرة الحدود $1+x+x^3$ لإنشاء $GF(2^3)$. فُك تشفير كل من الكلمات المستقبلة التالية التي تم تشفيرها باستخدام الشفرة $\widehat{C'}$ والخوارزمية (**٦,٦,٦**).

(أ) 0000 0000 1001 0011 1111 1010 1011.

(ب) 1001 0011 1010 0011 1000 0000 1011.

(ج) 0101 1100 1100 1100 0000 1000 0101.

(د) 0000 1001 0111 1101 1011 1010 0000.

(**٦,٦,١٠**) استخدم الشفرة $\widehat{C'}$ المقدمة في المثال (**٦,٦,٧**) والخوارزمية (**٦,٦,٦**) لفك تشفير الكلمات المستقبلة التالية :

(أ) $0\cdots0$ 10100 10100 10100 11110 00111 11010 11110 11101.

(ب) $0\cdots0$ 00101 10001 00000 11011 11111 01010 00000 11000.

(ج) $0\cdots0$ 10100 11101 10100 00101 10000 10000 10000 00000.

(**٦,٦,١١**) لتكن C هي الشفرة $RS(2^4,7)$ ولتكن $g(x) = (\beta+x)\cdots(\beta^6+x)$ كثيرة الحدود المولّدة حيث استخدمت كثيرة الحدود $1+x+x^4$ لإنشاء الحقل $GF(2^4)$. فُك تشفير الكلمة المستقبلة التالية إذا علمت أن الشفرة التي استخدمت في عملية التشفير $\widehat{C'}$ هي :

$0\cdots0$ 10000 11110 11101 01001 11011 10001 11011 01011.

الفصل السابع

شفرات تصويب الأخطاء الاندفاعية

Burst Error-Correcting Codes

(٧,١) مقدمة

Introduction

لغاية الآن كان اهتمامنا منصباً على تصميم شفرات تصويب أخطاء موزّعة عشوائياً. ولكن هناك بعض القنوات التي تسمح بحدوث أخطاء قريبة من بعضها بعضاً. على سبيل المثال، من الممكن أن يكون مصدر التشويش على قرص مدمج هو خدش على ذلك القرص ومن ثم فجميع الإحداثيات الواقعة على ذلك الخدش قد تبدلت أو قد تم مسحها مما يتسبب بمجموعة من الأخطاء القريبة بعضها من بعض. كما أن بقع ضوء الشمس تتسبب في وقوع أخطاء قريبة من بعضها بعضاً في الرسائل المرسلة من الأقمار الصناعية إلى الأرض. نُسمي مثل هذه الأخطاء التي تحدث بهذه الصورة أخطاء اندفاعية (أو أخطاء مفاجئة).

لنفرض أنه يمكن تحليل كثيرة الحدود $e(x)$ المقابلة للكلمة e على النحو $e(x) = x^k e'(x)$ حيث $e'(0) = 1$. عندئذ، نقول إن **طول اندفاع** e **(Burst Length of e)** هو $deg(e'(x)) + 1$. وبهذا فطول الاندفاع هو عدد الإحداثيات من أول وقوع للإحداثي 1 في e إلى آخر وقوع للإحداثي 1 في e.

هناك مفهوم مرادف وهو **طول الاندفاع الدوري (Cyclic Burst Length)** لكلمة e حيث يكون طول الاندفاع الدوري للكلمة $e \epsilon K^n$ يساوي ℓ إذا كانت الدرجة الصغرى لكثيرات الحدود $x^k e(x)(mod 1 + x^n)$ حيث $k = 0,1,\cdots,n-1$ هي $\ell - 1$.

مثال (٧,١,١)

لنفرض أن $n = 7$ وأن $e = 0101100$. عندئذ،

$$e(x) = x + x^3 + x^4 = x(1 + x^2 + x^3)$$

وبهذا تكون $e'(x) = 1 + x^2 + x^3$ و $e'(0) = 1$. إذن، طول اندفاع e يساوي $3 + 1 = 4$. (لاحظ أنه من الممكن الحصول على طول الاندفاع بعدّ الإحداثيات بين أول وقوع للإحداثي 1 وآخر وقوع للإحداثي 1 في الكلمة e). لايجاد طول الاندفاع الدوري يتوجب علينا حساب $x^k e(x)(mod 1 + x^7)$ لكل $k = 0,1,2,\cdots,6$ وإيجاد كثيرة الحدود الأصغر درجة من بينها. من السهل أن نرى أن $x^6 e(x)(mod 1 + x^7)$ هي كثيرة الحدود الأصغر درجة ودرجتها تساوي 3. إذن، طول الاندفاع الدوري ℓ للكلمة e يحقق $\ell - 1 = 3$. وبهذا يكون $\ell = 4$.

أما إذا كانت $e = 1000100 \leftrightarrow 1 + x^4 = x^0(1 + x^4)$ فنرى أن طول الاندفاع للكلمة e هو $4 + 1 = 5$ ولكن $x^3(1 + x^4) \equiv 1 + x^3(mod 1 + x^7)$ هي كثيرة الحدود الأصغر درجة ومن ثم فطول الاندفاع الدوري للكلمة e هو $\ell = 3 + 1 = 4$. ▲

لحد الآن افترضنا أن نمط الخطأ الأرجح وقوعه هو نمط الخطأ ذو الوزن الأصغر حيث بنينا هذا الافتراض على أساس أن الأخطاء مُستقلة بعضها عن بعض. ولكن الوضع مختلف في معظم التطبيقات الحقيقية، ولهذا يتحتّم علينا تغيير إستراتيجية تصويب الأخطاء.

عند استخدامنا طريقة MLD للشفرات الخطيّة، اخترنا ممثّل المجموعة المشاركة ليكون الكلمة ذات الوزن الأصغر في تلك المجموعة المشاركة واعتبرنا أن هذه الشفرة

تصوّب الأخطاء من النوع t عندما تقع جميع الكلمات التي وزنها لا يزيد عن t في مجموعات مشاركة مختلفة لتلك الشفرة. ولكن لمعالجة تصويب الأخطاء الاندفاعية، نختار ممثّل المجموعة المشاركة لنمط الخطأ ليكون الكلمة ذات الطول الاندفاعي الأصغر بين كلمات تلك المجموعة المشاركة. ولهذا نقول إن الشفرة الخطيّة **تصوّب الأخطاء الاندفاعية من النوع ℓ** (**ℓ-Burst Error Correcting Code**) إذا وقعت جميع الكلمات التي طولها الاندفاعي لا يزيد عن ℓ في مجموعات مشاركة مختلفة لتلك الشفرة. بصورة عامة، إذا كانت C تصوّب أخطاء من النوع t وتصوّب أخطاء اندفاعية من النوع ℓ فإن $t \leq \ell$ (لماذا ؟) ومن الممكن أن تكون هذه المتباينة فعلية (انظر التمارين (**٧,١,٥**)، (**٧,١,٦**)، (**٧,١,٧**)). بصورة مماثلة نقول إن الشفرة الخطيّة **تصوّب أخطاء اندفاعية دورية من النوع ℓ** (**ℓ-Cyclic Burst Error Correcting Code**) إذا وقعت جميع الكلمات التي طولها الاندفاعي الدوري لا يزيد عن ℓ في مجموعات مشاركة مختلفة لتلك الشفرة.

مثال (٧,١,٢)

اعتبر جميع أنماط الأخطاء الاندفاعية الدورية غير الصفرية التي طولها لا يزيد عن 3 في K^{15}. كل نمط خطأ من هذه الأنماط هو على الصورة $e(x) = x^k e'(x)$ ، $k = 0,1,\cdots,14$ حيث $e'(x) \epsilon \{1, 1+x, 1+x^2, 1+x+x^2\}$. ولهذا يكون عدد أنماط الأخطاء هذه هو $4 \times 15 = 60$. ▲

مثال (٧,١,٣)

افرض أن $g(x) = 1 + x + x^2 + x^3 + x^6$ كثيرة حدود مولّدة لشفرة خطيّة دورية من الطول 15 والبُعد 9. من الواضح أن هذه الشفرة لا تصوّب 3 أخطاء؛ وذلك لوجود 576 كلمة من وزن لا يزيد عن 3 وعدد المجموعات المشاركة يساوي 64 فقط. ولكن عدد أنماط الخطأ التي طول اندفاعها الدوري لا يزيد عن 3 يساوي 61 (انظر المثال (**٧,١,٢**)). ولذا من المحتمل أن تصوّب هذه الشفرة أخطاء اندفاعية

من النوع 3 (في الحقيقة هي كذلك، انظر التمرين (**٧,١,٤**)). حيث يمكن التحقق من ذلك بحساب تناذرات $x^k e'(x)(mod\ g(x))$ ، $k = 0,1,\cdots,14$ حيث $e'(x)\epsilon\{1,1+x,1+x^2,1+x+x^2\}$. ▲

تمارين

(**٧,١,٤**) تحقق من أن أنماط الأخطاء الاندفاعية الدورية ذات الطول 3 في K^{15} تنتمي إلى مجموعات مشاركة مختلفة للشفرة المقدمة في المثال (**٧,١,٣**).

(**٧,١,٥**) أثبت أن $g(x) = 1 + x^2 + x^4 + x^5$ تولّد شفرة خطيّة دورية C من الطول 15 وتصوّب أخطاء اندفاعية دورية من النوع 2. هل تصوّب C أخطاء من النوع 2 ؟

(**٧,١,٦**) أثبت أن $g(x) = 1 + x^3 + x^4 + x^5 + x^6$ تولّد شفرة خطيّة دورية C من الطول 15 وتصوّب أخطاء اندفاعية دورية من النوع 3. هل تصوّب C أخطاء من النوع 3 ؟ (**إرشاد**: استخدم حد هامينغ).

(**٧,١,٧**) أثبت أن $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ تولّد شفرة خطيّة دورية من الطول 15 وتصوّب أنماط أخطاء من النوع 2 وتصوّب أيضاً أنماط أخطاء اندفاعية دورية من النوع 4.

إذا كانت الشفرة C تصوّب أخطاء من النوع t وتصوّب أخطاء اندفاعية من النوع ℓ فلقد لاحظنا سابقاً أن $t \le \ell$. تقدم لنا المبرهنة التالية حداً أعلى لقيمة ℓ. من الممكن تقديم حد أعلى أفضل من الحد الأعلى الذي تقدمه المبرهنة (انظر التمرين (**٧,١,١٠**)) ولكن الحد الأعلى الذي تقدمه هذه المبرهنة يفي بالغرض.

مبرهنة (٧,١,٨)

إذا كانت C شفرة خطيّة من الطول n والبُعد k وتصوّب أخطاء اندفاعية من النوع ℓ فإن $\ell \le n - k$.

البرهان

لنفرض أن C شفرة خطيّة من النوع (n,k) وتصوّب أنماط أخطاء اندفاعية من النوع ℓ. عندئذ، تقع جميع أنماط الأخطاء الاندفاعية ذات الطول الذي لا يزيد عن ℓ في مجموعات مشاركة مختلفة. من ذلك نرى عدم وجود كلمتين حيث أول ℓ من إحداثيات كل منها يساوي 1 بحيث تقعان في مجموعة مشاركة واحدة. ولكن عدد هذه الكلمات يساوي 2^ℓ. ومن ثم عدد المجموعات المشاركة هو على الأقل 2^ℓ. وبهذا يكون $\ell \leq n-k$. ■

تمارين

(**٧,١,٩**) تحقق من أن الشفرات المقدمة في التمارين (**٧,١,٥**)، (**٧,١,٦**)، (**٧,١,٧**) تحقق الحد الأعلى المقدم في المبرهنة (**٧,١,٨**).

(**٧,١,١٠**) إذا كانت C شفرة خطيّة من النوع (n,k) وتصوّب أنماط أخطاء اندفاعية من النوع ℓ فأثبت أن $\ell \leq (n-k)/2$ [**إرشاد:** أثبت إمكانية كتابة أي نمط خطأ اندفاعي من الطول 2ℓ كمجموع نمطي خطأ بطول اندفاعي $e_1 \leq \ell$ و $e_2 \leq \ell$ على التوالي ومن ثم أثبت أن $e_1 + e_2 \notin C$].

إذا كانت C شفرة خطيّة دورية فتوجد خوارزمية فك تشفير فعّالة لتصويب أنماط الأخطاء الاندفاعية الدورية. لنفرض إذن أن C تصوّب أنماط أخطاء اندفاعية دورية من النوع ℓ ومولّدة بكثيرة حدود $g(x)$ من الدرجة $n-k$. من النقاش المقدم قبل المثال (**٤,٣,٧**) نرى أن:

$$H = \begin{bmatrix} r_0 \\ r_1 \\ \vdots \\ r_{n-1} \end{bmatrix} = \begin{bmatrix} I_{n-k} \\ r_{n-k} \\ r_{n-k+1} \\ \vdots \\ r_{n-1} \end{bmatrix}$$

هي مصفوفة اختبار النوعية للشفرة C حيث $1 \leq i \leq n-1$ ، r_i هي الكلمة من الطول $n-k$ التي تقابل كثيرة الحدود $r_i(x) \equiv x^i (mod\ g(x))$. ولقد بيّنا أيضاً

(باستخدام المصفوفة H) أنه إذا كانت $w(x) = c(x) + e(x)$ هي الكلمة المستقبلة فيكون التناذر للكلمة $w \leftrightarrow w(x)$ هو:

$$wH = s \leftrightarrow s(x) \equiv w(x)(mod\ g(x))$$

الحقيقتان التاليتان هما السبب الذي يجعل استخدام C و H فعّالاً عند فك تشفير أنماط الأخطاء الاندفاعية الدورية:

(١) إذا كان $e \leftrightarrow e(x)$ نمط خطأ طوله الاندفاعي لا يزيد عن ℓ فنرى استناداً إلى المبرهنة (٧,١,٨) أن $\ell \leq n-k$. ولذا يوجد i ، في الفترة $0 \leq i \leq n-1$ بحيث تقع جميع الإحداثيات 1 من الإزاحة الدورية e_i للكلمة e في البداية (أي أن $e_i \leftrightarrow x^ie(x)(mod 1 + x^n)$ ذات درجة أصغر من ℓ).

(٢) من السهل حساب تناذر الإزاحة الدورية w_i للكلمة w لأن:

$$\begin{aligned} s_i &= w_iH \\ &\leftrightarrow (x^iw(x)(mod 1 + x^n))mod g(x) \\ &\equiv x^iw(x)(mod g(x)) \qquad \text{(لأن } g(x) \text{ تقسم } 1 + x^n\text{)} \\ &\equiv x^is(x)(mod\ g(x)) \end{aligned}$$

ولهذا يكون تصويب الخطأ $w = c + e$ على النحو التالي:

لكل i ، $0 \leq i \leq n-1$ نقوم بحساب التناذرات $s_i \leftrightarrow x^is(x)(mod\ g(x))$ للكلمة w_i بالتالي حتى نجد واحداً وليكن s_j يحقق $deg(s_j(x)) < l$ حيث استخدمنا الحقيقة (٢) في هذه الحسابات. الآن، بما أن أول $n-k$ من صفوف H هي المصفوفة المحايدة فنرى أن تناذر الكلمة $e_j = s_j00\cdots0$ (التي نحصل عليها من s_j باضافة k من الأصفار إلى s_j) هو $e_jH = s_j$. وبما أن C دورية فنعلم أن $w_j = c_j + e_j$ حيث c_j هي كلمة الشفرة التي نحصل عليها من الإزاحة j الدورية للكلمة c. ومن ثم نستطيع إزاحة e_j إلى الخلف بعدد j من الإزاحات الدورية لنحصل على $e = e_0$. وهذا هو نمط الخطأ الاندفاعي الدوري. من ذلك نحصل على الخوارزمية التالية:

خوارزمية (٧,١,١١) [فك تشفير أنماط أخطاء اندفاعية دورية]

لنفرض أن w كلمة مُستقبلة تم تشفيرها باستخدام شفرة خطيّة دورية تصوّب أنماط أخطاء اندفاعية دورية من النوع ℓ حيث $g(x)$ هي كثيرة حدود مولّدة للشفرة.

(١) احسب كثيرة حدود التناذر $s(x) \equiv w(x)(mod\ g(x))$.

(٢) لكل $i \geq 0$ ، احسب $s_i(x) \equiv x^i s(x)(mod\ g(x))$ حتى تجد كثيرة حدود تناذر $s_j(x)$ تحقق $deg(s_i(x)) \leq \ell - 1$.

عندئذ، يكون نمط الخطأ الاندفاعي الدوري الأرجح وقوعاً هو:

$e(x) \equiv x^{n-j} s_j(x)(mod 1 + x^n)$.

مثال (٧,١,١٢)

لنفرض أن $g(x) = 1 + x + x^2 + x^3 + x^6$ كثيرة حدود مولّدة لشفرة خطيّة دورية من الطول 15 وتصوّب أنماط أخطاء اندفاعية دورية من النوع 3. استخدم الخوارزمية (**٧,١,١١**) لفك تشفير الكلمة المستقبلة 111100100001010 على افتراض أرجحية وقوع أنماط أخطاء اندفاعية دورية.

الحل

(١)
$$s(x) \equiv 1 + x + x^2 + x^3 + x^6 + x^{11} + x^{13}(mod\ g(x))$$
$$\equiv 1 + x^3 + x^4 + x^5$$

(٢)
$$s_1(x) \equiv xs(x)\big(mod\ g(x)\big) = 1 + x^2 + x^3 + x^4 + x^5$$
$$s_2(x) \equiv x^2 s(x)\big(mod\ g(x)\big) = 1 + x^2 + x^4 + x^5$$
$$s_3(x) \equiv x^3 s(x)\big(mod\ g(x)\big) = 1 + x^2 + x^5$$
$$s_4(x) \equiv x^4 s(x)\big(mod\ g(x)\big) = 1 + x^2$$

وإن $deg(s_4(x)) = 2 \leq \ell - 1$. إذن، نمط الخطأ الأرجحي هو:

$$e(x) \equiv x^{15-4} s_4(x)(mod(1 + x^{15}))$$
$$= x^{11} + x^{13}$$

ومن ثم تكون كلمة الشفرة الأرجح هي:

$$c(x) = w(x) + e(x) = 1 + x + x^2 + x^3 + x^6$$
$$\leftrightarrow 111100100000000. \quad \blacktriangle$$

تمارين

(**٧,١,١٣**) لنفرض أن $g(x) = 1 + x + x^2 + x^3 + x^6$ كثيرة حدود مولّدة لشفرة خطيّة دورية C من الطول 15 وتصوّب أنماط أخطاء اندفاعية دورية من النوع 3. فُك تشفير كل من الكلمات المستقبلة التالية التي شُفّرت بواسطة الشفرة C:

(أ) 101101110001000 (ب) 001101100010101

(ج) 100110101010011 (د) 101101000010111

(هـ) 000000111110000.

(**٧,١,١٤**) افرض أن $g(x) = 1 + x^2 + x^4 + x^5$ كثيرة حدود مولّدة لشفرة خطيّة دورية C من الطول 15 وتصوّب أنماط أخطاء اندفاعية دورية من النوع 2. فُك تشفير كل من الكلمات المستقبلة التالية التي شُفّرت بواسطة الشفرة C:

(أ) 010101000010010 (ب) 011010010010100

(ج) 001101000000100 (د) 000100010100101

(هـ) 000000011111001.

تتمتع شفرات ريد وسولومن بقدرة جيدة على تصويب الأخطاء الاندفاعية. تذكر أنه إذا كانت C هي الشفرة $RS(2^r, \delta)$ فإن $\hat{C}$ هي التمثيل الثنائي للشفرة C (انظر المثال (**٦,٢,٦**)).

مبرهنة (٧,١,١٥)

لتكن C هي الشفرة $RS(2^r, 2t + 1)$. عندئذ، $\hat{C}$ شفرة تصوّب أنماط أخطاء اندفاعية من النوع ℓ حيث $\ell \geq r(t - 1) + 1$.

البرهان

ينتج عن أي نمط خطأ اندفاعي e طوله لا يزيد عن $r(t-1)+1$ كلمة $\hat{w}=\hat{c}+e$ حيث $d(w,c)\leq t$. إذن، يكون فك تشفير w هي كلمة الشفرة $c\epsilon RS(2^r,2t+1)$. وبهذا تكون $\hat{c}\epsilon\hat{C}$ هي أقرب كلمة شفرة للكلمة $\hat{w}$. ■

تستخدم شفرات ريد وسولومن في الأقراص الممغنطة حيث تتسبب الخدوش على القرص بحدوث أخطاء اندفاعية. كما أنها تستخدم أيضاً في الاتصالات الفضائية من قبل NASA و ESA حيث تتسبب بقع ضوء الشمس بحدوث أخطاء اندفاعية أثناء عملية الإرسال التي تكون على شكل موجات كهرومغناطيسية. وفي كلتا الحالتين يفضّل أن نفترض أن الأخطاء التي وقعت هي أخطاء اندفاعية وليست أخطاء عشوائية.

مثال (٧,١,١٦)

تصوّب الشفرة $RS(8,5)$ المقدمة في التمرين (٦,٢,٨) جميع الأخطاء الاندفاعية التي طولها لا يزيد عن $r(t-1)+1=4$. ▲

(٧,٢) التوريق البيني
Interleaving[(١)]

إحدى طرق تحسين قدرة الشفرات على تصويب الأخطاء الاندفاعية هي استخدام تقنية التوريق البيني حيث تكمن فكرة هذه التقنية باعادة ترتيب إرسال إحداثيات كلمة الشفرة. الطريقة التي اتبعناها حتى الآن في إرسال الرسائل $m_1,m_2,\cdots$ كانت عبارة عن تشفير هذه الرسائل إلى كلمات شفرة مقابلة $c_1,c_2,\cdots$ ومن ثم إرسال كلمات الشفرة واحدة بعد الأخرى بهذا الترتيب. لنفرض الآن أننا قمنا باختيار أول s كلمة من

---

(١) المترجمان: الترجمة الحرفية للكلمة interleave هي يورق بينياً. أي يضع ورقة بيضاء بين ورقتي كتاب. ولهذا نرى أنها ترجمة مناسبة لموضوع هذا البند.

كلمات الشفرة ثم بعد ذلك قمنا بإرسال أول إحداثي من كل كلمة من هذه الكلمات، بعد ذلك قمنا بإرسال ثاني إحداثي من كل كلمة من هذه الكلمات وهكذا. وبمجرد الانتهاء من إرسال الإحداثيات التي عددها ns من أول s كلمة من كلمات الشفرة بالترتيب المبيّن نقوم باختيار مجموعة جديدة من كلمات الشفرة عددها s ونكرّر عملية إرسال الإحداثيات بالترتيب نفسه للمجموعة الأولى. وهكذا إلى أن ننتهي من عملية الإرسال. تُسمى إعادة ترتيب إحداثيات كلمات الشفرة بهذا الأسلوب، **التوريق البيني بعمق s** (**Interleaving to Depth s**). يمكن صياغة التوريق البيني لكلمات الشفرة $c_1, c_2, \cdots$ لعمق s على النحو التالي:

لكل $i = 0,1,2,\cdots$ نقوم بإرسال إحداثيات كلمة الشفرة بالترتيب التالي:

$c_{is+1}, 1, c_{is+2}, 1, \cdots, c_{is+s}, 1, c_{is+1}, 2, c_{is+2}, 2, \cdots, c_{is+s}, 2, \cdots, c_{is+1}, n, \cdots, c_{is+s}, n,$.

ولتسهيل رؤية عملية الإرسال هذه نقوم بكتابة كلمات الشفرة $c_{is+1}, \cdots, c_{is+s}$ على شكل صفوف (انظر الجدول (٧,١)) ثم ارسال الإحداثيات عموداً عموداً.

الجدول (٧,١). توريق بيني لعمق s.

$$\begin{matrix} c_{is+1,1} & c_{is+1,2} & c_{is+1,3} & \cdots & c_{is+1,n} \\ c_{is+2,1} & c_{is+2,2} & c_{is+2,3} & \cdots & c_{is+2,n} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{is+s,1} & c_{is+s,2} & c_{is+s,3} & \cdots & c_{is+s,n} \end{matrix}$$

مثال (٧,٢,١)

لتكن C شفرة خطية ذات مصفوفة مولّدة $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. إذا لم يستخدم التوريق البيني فيتم ارسال كلمات الشفرة التالية:

$$\begin{aligned} c_1 &= 100110, \quad c_4 = 010101 \\ c_2 &= 010101, \quad c_5 = 100110 \\ c_3 &= 111000, \quad c_6 = 111000 \end{aligned}$$

كلمة بعد الأخرى ومن ثم فإحداثيات الشفرة تُرسل بالترتيب التالي:

.100110 010101 111000 010101 100110 111000

أما إذا استخدمنا التوريق البيني لعمق 3 فنقوم بإرسال الإحداثيات الأولى من كلمات الشفرة c_1, c_2, c_3 أولاً (أي 101) وبعد ذلك نُرسل الإحداثي الثانية من كلمات الشفرة c_1, c_2, c_3 (أي 011) وهكذا. وبهذا يتم إرسال إحداثيات الكلمات c_1, c_2, c_3 على النحو التالي:

.011 101 001 110 010 100 ▲

ما هو تأثير التوريق البيني لعمق s على قدرة تصويب الشفرة C لأنماط الأخطاء الاندفاعية؟ لرؤية ذلك، نفرض أن ترتيب إرسال الإحداثي الأول من كلمة الشفرة c هو i. حينئذ، تكون مواقع بقية إحداثيات الكلمة c هي $i + s, i + 2s, \cdots, i + (n-1)s$. لنفرض أن C شفرة تصوّب أخطاء اندفاعية من النوع ℓ. إذا استخدمنا التوريق البيني لعمق s للشفرة C فنرى إن أي اندفاع للأخطاء أثناء عملية الإرسال طوله لا يزيد عن $s\ell$ ينتج عنه نمط خطأ اندفاعي في كلمة الشفرة c طوله لا يزيد عن ℓ، وبهذا يكون فك تشفير c صحيحاً بحالة عدم وجود أنماط أخطاء اندفاعية أخرى تؤثر في c. وبهذا نكون قد برهنا النتيجة التالية:

مبرهنة (٧,٢,٢)

لتكن C شفرة تصوّب أنماط أخطاء اندفاعية من النوع ℓ. إذا تم توريق C بينياً لعمق s فإنه يتم تصويب جميع أنماط الأخطاء الاندفاعية التي طولها لا يزيد عن $s\ell$ بافتراض أن كل كلمة شفرة تأثّرت على الأكثر باندفاع أخطاء واحد. ■

ملحوظة

إن الشرط الاحترازي بعدم تأثر كل من كلمات الشفرة بأكثر من اندفاع واحد من الأخطاء يفترض وجود مسافة كافية بين كل نمطين من أنماط الأخطاء الاندفاعية

أثناء عملية الإرسال لتجنب تأثير نمطين من الأخطاء الاندفاعية على قالب واحد طوله s من كلمات الشفرة. ولهذا فإن اختيار عدد كبير s يزيد من ضمان تصويب أنماط الأخطاء الاندفاعية تحت شروط المبرهنة (٧,٢,٢)، كما أنه يضمن وجود مسافة كافية بين أنماط الأخطاء الاندفاعية أثناء الإرسال.

مثال (٧,٢,٣)

تصوّب الشفرة C المقدمة في المثال (٧,٢,١) خطأً واحداً. إذا تم توريقها بينياً لعمق 3 فهذا يزيد من قدرتها بحيث تستطيع تصويب أنماط أخطاء اندفاعية من الطول 3. ▲

تمارين

(٧,٢,٤) شفّر الرسائل $m_1 = 1000$ ، $m_2 = 0110$ ، $m_3 = 1110$ ، $m_4 = 0011$ ، $m_5 = 0110$ ، $m_6 = 0001$. جد أيضاً الإحداثيات المرسلة إذا تم توريق الشفرة لعمق s حيث:

$$G = \begin{bmatrix} 1000110 \\ 0100101 \\ 0010011 \\ 0001111 \end{bmatrix}$$

(أ) $s = 1$ (ب) $s = 2$ (ج) $s = 3$.

(٧,٢,٥) ذكرنا في المثال (٧,١,٣) أن كثيرة الحدود $g(x) = 1 + x + x^2 + x^3 + x^6$ تولّد شفرة خطية دورية C من الطول 15 ولها القدرة على تصويب أنماط أخطاء اندفاعية دورية من النوع 3. استخدم المصفوفة G المولّدة للشفرة C:

$$G = \begin{bmatrix} 111100100000000 \\ 011110010000000 \\ \vdots \\ 000000001111001 \end{bmatrix}$$

لتشفير الرسائل $m_1(x) = 1$ ، $m_2(x) = x^2$ ، $m_3(x) = 1 + x$ ، $m_4(x) = 1 + x^2$ ، $m_5(x) = x^3$ ، $m_6(x) = 1$. جد الإحداثيات المرسلة إذا تم توريق C بينياً لعمق s حيث:

(أ) $s = 1$ (ب) $s = 2$ (ج) $s = 3$.

في كل من قيم S المعطاة، استخدم المبرهنة (٧,٢,٢) لتجد أي أنماط أخطاء اندفاعية تستطيع الشفرة تصويبها.

أحد عوائق التوريق البيني لعمق s هو ضرورة تشفير عدد s من كلمات الشفرة قبل الشروع في إرسال أي منها. للتغلب على هذا العائق نستخدم **الاطار المؤجل للتوريق البيني من النوع s** (**s-Frame Delayed Interleaving**)؛ وذلك بسرد إحداثيات كل من كلمات الشفرة كما هو مبيّن في الجدول (٧,٢) (قارن ذلك مع الجدول (٧,١)). ومن ثم نقوم بارسال الإحداثيات عموداً عموداً. يحتوي صفيف الجدول (٧,٢) على عدد n من الصفوف. لكل كلمة شفرة c_i يوجد إحداثي واحد فقط $c_{i,j}$ في الصف j $(1 \leq i \leq n)$ حيث $c_{i,j+1}$ تقع في الصف الذي يقع مباشرة أسفل الصف الذي يقع فيه الإحداثي $c_{i,j}$ وتبعد عدد s من الأعمدة عن العمود الواقع فيه الإحداثي $c_{i,j}$ $(1 \leq j \leq n-1)$.

الجدول (٧,٢). اطار مؤجل للتوريق البيني من النوع s.

$c_{1,1}c_{2,1}\cdots$	$c_{s+1,1}$	$c_{s+2,1}\cdots$	$c_{2s+1,1}$	$c_{2s+2,1}$	$\cdots$	$c_{(n-1)s+1,1}$	$\cdots$
	$c_{1,2}$	$c_{2,2}\cdots$	$c_{s+1,2}$	$c_{s+2,2}$	$\cdots$	$c_{(n-2)s+1,2}$	$\cdots$
			$c_{1,3}$	$c_{2,3}$	$\cdots$	$c_{(n-3)s+1,3}$	$\cdots$
						$\vdots$	
						$c_{1,n}$	$\cdots$

من الواضح أن استخدام الاطار المؤجل للتوريق البيني من النوع s يحتاج إلى بعض التحضير؛ لأنه إذا كان $s \geq 1$ فإن العمود الأول من الجدول (٧,٢) يحتوي فقط إحداثياً واحداً هو $c_{1,1}$، ولضمان وجود عدد n من الإحداثيات في كل من أعمدة الجدول (٧,٢) نقوم بوضع الإحداثي 0 في المواضع الخالية من الإحداثيات. المثال التالي يوضح ذلك مع ملاحظة وضع * عوضاً عن 0 في المواضع الخالية؛ وذلك لتفريقها عن الإحداثي 0 من كلمة الشفرة.

مثال (٧,٢,٦)

لتكن $c_1, c_2, \cdots, c_6$ هي كلمات الشفرة المبينة في المثال (٧,٢,١). إذا استخدمنا إطاراً مؤجلاً للتوريق البيني من النوع 1 فيكون الجدول (٧,٢) على النحو التالي:

$$\begin{array}{cccccccccccc}
1 & 0 & 1 & 0 & 1 & 1 & \cdots \\
* & 0 & 1 & 1 & 1 & 0 & 1 & \cdots \\
* & * & 0 & 0 & 1 & 0 & 0 & 1 & \cdots \\
* & * & * & 1 & 1 & 0 & 1 & 1 & 0 & \cdots \\
* & * & * & * & 1 & 0 & 0 & 0 & 1 & 0 & \cdots \\
* & * & * & * & * & 0 & 1 & 0 & 1 & 0 & 0 & \cdots
\end{array}$$

حيث قمنا بداية بوضع * في المواقع الخالية من الأعمدة. ومن ثم يتم الإرسال على النحو التالي:

$$1 ***** 00 **** 110 *** 0101 ** \cdots.$$

أما إذا استخدمنا إطاراً مؤجلاً للتوريق البيني من النوع 2 فيكون الجدول (٧,٢) على النحو التالي:

$$\begin{array}{ccccccccccccccccc}
1 & 0 & 1 & 0 & 1 & 1 & \cdots \\
* & * & 0 & 1 & 1 & 1 & 0 & 1 & \cdots \\
* & * & * & * & 0 & 0 & 1 & 0 & 0 & 1 & \cdots \\
* & * & * & * & * & * & 1 & 1 & 0 & 1 & 1 & 0 & \cdots \\
* & * & * & * & * & * & * & * & 1 & 0 & 0 & 0 & 1 & 0 & \cdots \\
* & * & * & * & * & * & * & * & * & * & 0 & 1 & 0 & 1 & 0 & 0 & \cdots
\end{array}$$

ومن ثم يتم الإرسال على النحو التالي:

$$1 ***** 0 ***** 10 **** 01 **** 110 *** \cdots. \quad \blacktriangle$$

المبرهنة التالية هي رديف المبرهنة (٧,٢,٢) في حالة استخدام اطار مؤجل للتوريق البيني من النوع s.

مبرهنة (٧,٢,٧)

لتكن C شفرة تصوّب أخطاء اندفاعية من النوع ℓ. إذا كانت C تستخدم إطاراً مؤجلاً للتوريق البيني من النوع s فإن C تصوّب جميع الأخطاء الاندفاعية من النوع $\ell(sn+1)$ بشرط أن تكون كل كلمة شفرة قد تأثرت على الأكثر باندفاع واحد من الأخطاء.

تمارين

(٧,٢,٨) استخدم إطاراً مؤجلاً للتوريق البيني من النوع s وكلمات الشفرة المقدمة في التمرين (٧,٢,٤) لايجاد الإحداثيات المرسلة عندما يكون

(أ) $s = 1$ (ب) $s = 2$.

(٧,٢,٩) إذا استخدم اطار مؤجل للتوريق البيني من النوع 0 فما هي الإحداثيات المرسلة ؟

(٧,٢,١٠) أثبت المبرهنة (٧,٢,٧).

عند التطبيق العملي تستخدم شفرتان لتشفير الرسائل. على سبيل المثال، تستخدم شفرتان لتشفير النغمات الموسيقية على الأقراص الممغنطة (انظر البند (٧,٣)) والشفرتان هما شفرات ريد وسولومن. كما تستخدم كل من NASA و ESA شفرتين إحداهما شفرة ريد وسولومن والأخرى شفرة تلاف (انظر البند (٨,٢))، وكما سنرى الآن، يلعب التوريق البيني لعمق s أهمية خاصة في مثل عمليات التشفير هذه المكوّنة من خطوتين.

افرض أن C_1 شفرة خطية من النوع (n_1, k_1, d_1) و C_2 شفرة خطية من النوع (n_2, k_2, d_2). يتم استخدام التوريق البيني في تشفير C_1 و C_2 على النحو التالي :

تُشفّر الرسائل أولاً باستخدام C_1 ومن ثم يستخدم التوريق البيني لعمق k_2 على كلمات الشفرات الناتجة. طول كل من الأعمدة الناتجة عن عملية التوريق البيني هذه هو k_2 (كما في الجدول (٧,١)) وبهذا ينظر إليها على أنها رسائل يتم تشفيرها باستخدام C_2. نقوم الآن بتوريق بيني لكلمات الشفرة الناتجة عن التشفير الثاني لعمق s أو لإطار مؤجل من النوع s.

الميزة الأساسية للتشفير بخطوتين هي :

يمكن استخدام C_2 لاكتشاف أخطاء عددها $d_2 - 1$ عوضاً عن استخدامها لتصويب أخطاء. عند اكتشاف أخطاء في احدى كلمات الشفرة C_2 نقوم بتعليم جميع إحداثيات هذه الكلمة ونتعامل معها على أنها إحداثيات غير صحيحة. بعد ذلك نركّز اهتمامنا على كلمات الشفرة C_1. إذا علمنا وجود $n_1 - d_1 + 1$ إحداثياً صحيحاً من إحداثيات كلمة شفرة $c \epsilon C_1$ فباستطاعتنا دائماً إيجاد بقية الإحداثيات التي عددها $d_1 - 1$. يرجع السبب وراء ذلك لاستحالة اتفاق كلمة أخرى من كلمات الشفرة C_1 مع الكلمة c بإحداثيات صحيحة عددها $n_1 - d_1 + 1$ ؛ لأن جميع كلمات الشفرة تختلف على الأقل بمواقع عددها d_1. إذن ، إذا احتوت كل من كلمات C_1 على عدد من الإحداثيات المعلّمة لا يزيد عن $d_1 - 1$ وإذا افترضنا أن جميع الإحداثيات الخاطئة قد تم تعليمها فنرى أنه قد تم فك تشفير كلمات الشفرة بصورة صحيحة.

مثال (٧,٢,١١)

لنفرض أن C_1 و C_2 شفرتان مصفوفتاهما المولدتان هما على التوالي :

$$G_1 = \begin{bmatrix} 10001110 \\ 01001101 \\ 00101011 \\ 00010111 \end{bmatrix} \text{ و } G_2 = \begin{bmatrix} 100110 \\ 010101 \\ 001011 \end{bmatrix}.$$

عندئذ، $(n_1, k_1, d_1) = (8,4,4)$ و $(n_2, k_2, d_2) = (6,3,3)$. سنقوم بتشفير الرسائل $m_1 = 1000$ ، $m_2 = 1100$ ، $m_3 = 1010$ باستخدام التوريق البيني بين C_1 و C_2 حيث ورقت C_2 بينياً لعمق $s = 3 = d_1 - 1$. باستخدام C_1 لتشفير m_1 ، m_2 ، m_3 نرى أن:

$$c_1 = m_1 G_1 = 10001110$$
$$c_2 = m_2 G_1 = 1100011$$
$$c_3 = m_3 G_1 = 10100101$$

بتوريق كلمات الشفرة هذه بينياً لعمق $k_2 = 3$ تكون الرسائل الناتجة عن أعمدة هذا التوريق هي:

.111,010,001,000,100,101,110,011

نستخدم الآن C_2 لتشفير هذه الرسائل لينتج عن ذلك 8 كلمات شفرة يتم توريقها بينياً لعمق $s = 3$ لينتج عن ذلك:

$c'_1 = 111000$ | $c'_4 = 000000$ | $c'_7 = 110011$

$c'_2 = 010101$ | $c'_5 = 100110$ | $c'_8 = 011110$

$c'_3 = 001011$ | $c'_6 = 101101$

(تورق c'_7 و c'_8 مع أول كلمة شفرة c'_9 التي تنتج عن الرسائل الثلاث التي تلي ذلك m_4, m_5, m_6). إذن، تكون بداية الإحداثيات المرسلة هي:

.100 110 101 010 001 011 011 000 001 011 010 001 $\cdots$

ولرؤية كيفية فك التشفير، نفرض أنه قد حصل خطأ في الإحداثيات الستة الأولى. أي أننا استقبلنا:

011 001 101 010 001 011 000 $\cdots$

بإلغاء تأثير التوريق البيني لعمق $s = 3$ ينتج عن ذلك كلمات مستقبلة طولها $n_2 = 6$:

001000,100101,111011

(لاحظ أنه بالمقارنة مع c'_1 ، c'_2 ، c'_3 على التوالي نرى أن كل منها يحتوي على أخطاء في أول موقعين). الآن، تكتشف C_2 الأخطاء في جميع الكلمات الثلاث هذه (أثبت أن التناذر wH_2 لكل من هذه الكلمات المستقبلة w لا يساوي صفراً حيث H_2 هي مصفوفة اختبار النوعية للشفرة C_2). وبهذا تكون الإحداثيات الـ 18 جميعها معلّمة (نستبدل كل منها بالعلامة *). بفرض عدم اكتشاف أخطاء أخرى بعد عملية مماثلة لإحداثيات كلمات الشفرة $c'_4, c'_5, \cdots, c'_8$ فنرى بعد إزالة تأثير التوريق البيني لعمق $k_3 = 3$ أننا قد حصلنا على ثلاث كلمات طول كل منها $n_1 = 8$:

$$c_1 = *** \ 01110$$
$$c_2 = *** \ 00011$$
$$c_3 = *** \ 00101$$

بعد ذلك توجد طريقة واحدة فقط للتعويض عن الإحداثيات المعلّمة * بأحد الإحداثيين 0 و 1 للحصول على كلمات شفرة c_1, c_2, c_3. لاحظ أن كلاً من الكلمات الثلاث السابقة تحتوي على إحداثيات معلّمة عددها $3 = d_1 - 1$. ▲

تمارين

(٧,٢,١٢) استخدم الشفرتين C_1 و C_2 لتشفير مجموعات الرسائل التالية مُستخدماً التوريق البيني بينهما إذا علمت أن التوريق البيني للشفرة C_2 هو لعمق s.

(أ) $m_1 = 0110, m_2 = 1011, m_3 = 1111, s = 2$

(ب) $m_1 = 0110, m_2 = 1011, m_3 = 1111, s = 3$

(ج) $m_1 = 0010, m_2 = 1111, m_3 = 1010, s = 3$

(د) $m_1 = 1000, m_2 = 0100, m_3 = 0010,$
$m_4 = 0001, m_5 = 0011, m_6 = 0100, s = 3$

(٧,٢,١٣) إذا علمت أن الإحداثيات التالية قد تم تشفيرها بتوريق بيني للشفرتين C_1 و C_2 المقدمتين في المثال (**٧,٢,١١**) حيث ورقت C_1 بينياً لعمق 3 فجد فك تشفير هذه الإحداثيات وذلك بإيجاد الرسائل m_1, m_2, m_3.

(أ) $\cdots$ 0000010011101100010001110001110001110000000000000000000

(ب) $\cdots$ 100011001111101010011001111010100110100100011101000100

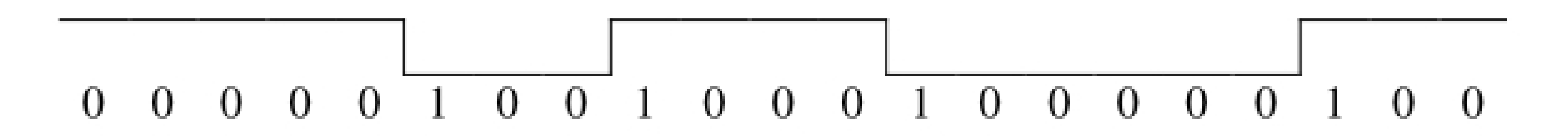
(٧,٢,١٤) لتكن $C_i = (n_i, k_i, d_i)$ حيث $i = 1,2$ شفرتين خطيتين. لنفرض أن C_1 ورقت بينياً مع C_2 للحصول على كلمات شفرة. جد طول الخطأ الاندفاعي الذي يمكن تصويبه باستخدام خوارزمية فك التشفير المقدمة في المثال (**٧,٢,١١**) إذا كانت كلمات الشفرة هذه:

(أ) ورقت بينياً لعمق s قبل إرسالها.

(ب) استُخْدِمِ مؤجل للتوريق البيني لعمق s قبل ارسالها.

(٧,٣) تطبيقات على الأقراص المدمجة
Applications to Compact Discs

أحدث استخدام الأقراص المدمجة لتسجيل الألحان الموسيقية تغييراً أساسياً في عالم الموسيقى، حيث إن السبب وراء الجودة العالية للألحان المسجلة على الأقراص المدمجة هو استخدام شفرات تصويب الأخطاء عند تخزين هذه الألحان. يتكون على القرص المدمج مسار حلزوني على نقرات أو ندب صغيرة (مستوى منخفض) ومن ثم يتبع ذلك حزمة من أشعة الليزر (أو اللازر) لتحديد التغيرات في ارتفاع المسار الحلزوني وذلك باكتشاف التغيرات في شدة كمية الضوء المنعكسة من القرص المدمج. ينتج عن ذلك كلمات ثنائية حيث يقابل كل تغير في الارتفاع الإحداثي 1 ويقابل عدم التغير في الارتفاع الإحداثي 0.



يتم أثناء عملية التسجيل أخذ 44100 عينة موسيقية في كل ثانية حيث يقابل سعة الموجة الصوتية لكل عينة كلمة ثنائية طولها 16. ولهذا يقسم مدى السعات إلى 2^{16} قيمة. تحتاج عملية التسجيل على **الستيريو (Stereo)** إلى قياسين للسعة يؤخذان 44100 مرة في كل ثانية، واحد من اليسار والآخر من اليمين.

لأغراض التشفير يتم تمثيل كل كلمة ثنائية طولها 16 التي تقابل قياس سعة بعنصرين في الحقل $GF(2^8)$ (يُطلق مصطلح بايت byte على كل عنصر من عناصر الحقل). أثناء عملية التسجيل يتم انتاج 4 بايتات هي m_{4t} ، m_{4t+1} ، m_{4t+2} ، m_{4t+3} عند كل **تكّة "tick"** t حيث قيمة التكّة تساوي $\frac{1}{44100}$ من الثانية. بعد ذلك يتم تجميع قياسات سعة من 6 تكّات متتالية $m_{24t}, m_{24t+1}, \cdots, m_{24t+23}$ للحصول على رسالة M_t طولها 24 حيث كل بايت ينتمي إلى $GF(2^8)$. لنفرض أن C هي الشفرة $RS(2^8, 5)$. عندئذ، يتم تشفير الرسالة M_t إلى كلمة شفرة c_t باستخدام الشفرة $C_1 = C(227)$ التي هي مقصور شفرة ريد وسولومن على الحقل $GF(2^8)$ حيث $(n_1, k_1, d_1) = (28,24,5)$ (انظر المثال (**٦,٢,١١**)).

بهذا نكون قد استخدمنا إطاراً مؤجلاً للتوريق البيني من النوع 4 لكلمات الشفرة التي حصلنا عليها (انظر الجدول (**٧,٢**)). لاحظ أن طول كل من أعمدة صفيف الجدول (**٧,٢**) في حالتنا هذه يساوي $n_1 = 28$. وبما أن البايتات في كلمة الشفرة c_t تقع في الأعمدة $t, t+4, t+8, \cdots, t+108$ فمن الطبيعي أن نرمز لهذه البايتات بالرموز $c_{1,t}, c_{2,t+4}, c_{3,t+8}, \cdots, c_{28,t+108}$.

يحتوي العمود t من صفيف الجدول (**٧,٢**) على البايتات $c_{1,t}, c_{2,t}, \cdots, c_{28,t}$ (تذكر أن $c_{i,j}$ هي البايت i في كلمة الشفرة $c_{j-4(i-1)}$)، وهذه قد استخدمت كرسائل من الطول 28 على الحقل $GF(2^8)$ ومن ثم شُفّرت باستخدام $C_2 = C(223)$ وهي شفرة ريد وسولومن المقصورة على $GF(2^8)$ حيث $(n_2, k_2, d_2) = (32,28,5)$.

يُضاف بايت لكل من كلمات الشفرة C_2 لغرض السيطرة والعرض ومن ثم يكون طول كلمات الشفرة يساوي 33.

جميع البايتات لحد الآن إما أنها تحمل معلومات وإما تم إضافتها لغرض اكتشاف وتصويب الأخطاء. ولكن يظهر عند التطبيق العملي لمسار الليزر أن التغيرات في ارتفاع المسار الحلزوني لا تقع قريبة جداً من بعضها بعضاً ولا بعيدة جداً بعضها عن بعض. ولهذا فقد تقرر أن يظهر على الأقل صفران وعلى الأكثر عشرة أصفار بين كل ظهورين متتاليين للواحد في التمثيل الثنائي لكلمة الشفرة. شفرة ريد وسولومن لا تتمتع بهذه الخاصية ولكن يوجد 267 كلمة ثنائية طول كل منها 14 تتمتع بهذه الخاصية. يتم مقابلة عناصر الحقل وعددها 256 مع 256 من هذه الكلمات الثنائية (توضع عادة في جدول) وتهمل 11 كلمة ثنائية. تُسمى هذه العملية، تغييراً في طبقة الصوت من ثمانية إلى أربعة عشر (اختصاراً EFM). ولغرض التأكد من أن هذه الخاصية تتحقق بين الكلمات من الطول 14 يُضاف 3 بايتات أخرى (إما كلها 0 وإما كلها 1). وبهذا يكون طول كل تمثيل بياني لكلمة شفرة يساوي $561 = 17 \times 33$.

وأخيراً، يُضاف لغرض المزامنة كلمة ثنائية طولها 27 لكل كلمة شفرة بحيث تبقى الخاصية المقدمة في الفقرة السابقة محققة. وبهذا يتم بداية تخزين المعلومات الصوتية لست تكّات متتالية كمتجه ثنائي طوله $196 = 8 \times 24$ وبعد إتمام جميع العمليات يظهر على القرص المدمج ككلمة ثنائية طولها 588.

يبقى علينا مناقشة فك التشفير. نقوم أولاً بمعالجة الخطوات الزائدة عكسياً مثل EFM على أمل أن تكون الكلمات المستقبلة هي كلمات شفرة تنتمي إلى C_1 (انظر الملحوظة في نهاية هذا البند). تستخدم الشفرة C_2 لتصويب خطأ واحد في جميع الكلمات. وإذا تم اكتشاف أكثر من خطأ فنقوم بتعليم جميع بايتات الكلمة المستقبلة (انظر البند (٧,٢) للتوريق البيني بين شفرتين). وبهذا يتم التخلص من تأثير الاطار

المؤجل للتوريق البيني من النوع 4. وأخيراً تستخدم الشفرة C_1 لتصويب أخطاء لا يزيد عددها عن 4 أخطاء (تذكر أن مسافة C_1 تساوي 5) على اعتبار أن جميع البايتات المعلّمة أخطاء والبايتات غير المعلّمة هي إحداثيات صحيحة.

هل فك التشفير هذا جيد؟ للاجابة عن ذلك، لاحظ أولاً أن الشرط الوحيد الذي ينتج عنه خطأ في استخدام C_2 لفك التشفير هو أن تكون المسافة بين الكلمة المستقبلة وكلمة شفرة تنتمي إلى C_2 ولكنها ليست الكلمة المرسلة لا تزيد عن 1. ولكن عدد أنماط الأخطاء التي تتمتع بهذه الخاصية قليل جداً؛ لأن عدد كلمات الشفرة C_2 هو $(2^r)^k = (2^8)^{28} = 2^{224}$ وواحدة فقط من هذه الكلمات هي الكلمة المنشودة وجميع الكلمات المتبقية وعددها $2^{224} - 1$ تقع على مسافة 1 من كلمات عددها $1 + 32(2^8 - 1)$ وطول كل منها يساوي 32. وبهذا نرى أنه من بين جميع أنماط الأخطاء الثنائية التي عددها $(2^8)^{32}$ المحتمل إضافتها إلى كلمة من كلمات الشفرة C_2 يوجد من بينها فقط عدد $(2^{224} - 1)(1 + 32(2^8 - 1))$ كلمة تقع على مسافة مقدارها 1 من كلمة أخرى من كلمات الشفرة C_2. أي أن هذا العدد هو تقريباً $1/2^{19}$ من هذه الكلمات. تم تصميم هذا الاستخدام للشفرة C_2 التي تصوّب نمط خطأ واحد لمعالجة الأخطاء العشوائية الصغيرة التي تحدث أثناء طلاء الأقراص المدمجة وقطعها.

أيضاً، بعد إزالة تأثير الاطار المؤجل للتوريق البيني من النوع 4 يتم فك تشفير الكلمة المستقبلة إلى كلمة شفرة صحيحة من كلمات C_1 إذا كان عدد الإحداثيات المعلّمة في الكلمة لا يزيد عن 4 (بافتراض أن C_2 تكتشف جميع الأخطاء وهذا هو الوضع في غالب الأحيان كما بيّنا سابقاً). ولكن قبل تأثير اندفاع واحد على 5 إحداثيات من كلمة في الشفرة C_1 يجب أن يؤثر على 17 عموداً من صفيف الجدول (٧,٢). أي على $15 \times 32 + 2 + 2$ بايتاً على الأقل (إذا تغير بايتان من العمود الأول أو العمود السابع عشر فينتج عن ذلك تعليم جميع بايتات هذا العمود بواسطة C_2).

وبما أن كل من أعمدة الجدول (٧,٢) يقابل كلمة طولها 588 على القرص المدمج فنرى أن جميع الاندفاعات من الطول $8871 = 17 \times 3 + 588 \times 15$ يتم فك تشفيرها بصورة صحيحة. يقابل هذا الطول الاندفاعي ما يقارب من $2.5mm$ من طول مسار على القرص المدمج.

ملحوظة

لاحظ أننا قمنا بتوضيح أوجه عملية التشفير المهمة فقط حيث توجد عمليات توريق بيني أخرى عند التطبيق العملي. على سبيل المثال، يتم إزاحة جميع البايتات التي تقع في مواقع فردية من كلمات الشفرة C_2 مواقع عددها $n_2 = 32$ بحيث يتم خلطها مع البايتات ذات المواقع الزوجية في كلمة الشفرة التالية مما يحسن من فرص قدرة الشفرة C_2 من تصويب نمط خطأ واحد؛ وذلك لأن خطأين متتاليين يؤثران الآن على كلمتي شفرة مختلفتين.

أيضاً، يتم إعادة ترتيب البايتات في كلمات الشفرة C_1. كل من هذه الكلمات يحتوي معلومات 6 تكّات متتالية من اليسار واليمين ولتكن $L_1, L_2, \cdots, L_6$ و $R_1, R_2, \cdots, R_6$ إضافة إلى رمزين للنوعية Q_1 و Q_2 يتم اضافتهما عند استخدام C_1 للتشفير. يتم ترتيب ذلك على النحو التالي:

$$L_1L_3L_5R_1R_3R_5Q_1Q_2L_2L_4L_6R_2R_4R_6$$

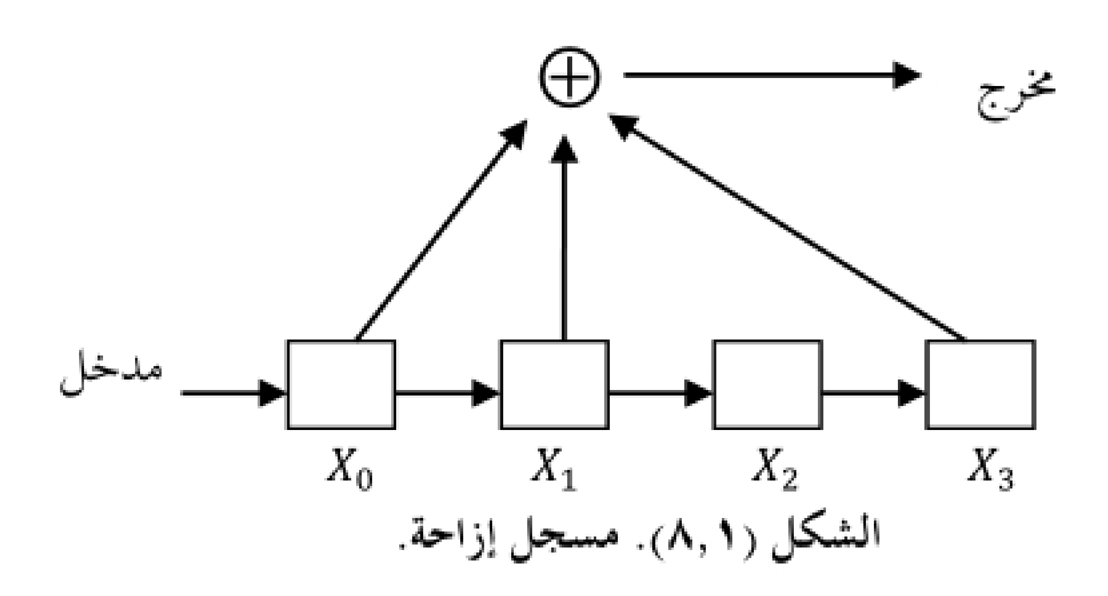
الغرض من ذلك هو أنه لو بقي عدد من البايتات المتتالية معلّماً بعد عملية فك التشفير فتعامل على أنها معلومات غير موثوقة. وفي هذه الحالة يمكن استبدال قيمة غير موثوق بها L_i بالسعة التي وجدت باستكمال القيمتين الموثوقتين L_{i-1} و L_{i+1}. على سبيل المثال، إذا بقيت القيم $L_1, L_5, R_1, R_3, R_5, Q_1, Q_2$ معلّمة فنستطيع إيجاد القيمة L_3 كوسط حسابي لسعتي القيمتين الموثوقتين L_2 و L_4 وهكذا.

الفصل الثامن

شفرات التلاف
Convolutional Codes

(٨,١) مسجلات الإزاحة وكثيرات الحدود
Shift Registers & Polynomials

أحد الأسباب التي تجعل للشفرات الدورية أهمية خاصة هي وجود أدوات فعّالة لتنفيذ عمليتي تشفير وفك تشفير كثيرات الحدود، تُدعى **مسجلات الإزاحة (Shift Registers)**. يتكون مسجل الإزاحة من عدد n من المسجلات (أو عناصر تأخير) وساعة وظيفتها التحكم في حركة أو إزاحة البيانات الموجودة على المسجلات. بعد كل تكّة من تكّات الساعة تجري عملية جمع ثنائية على المحتويات الجديدة للمسجلات لنحصل على مخرج. ففي الشكل (٨,١)، المربعات تمثل المسجلات، المتجهات تمثل اتجاه تدفق البيانات وأخيراً $\oplus$ هي عملية الجمع الثنائي.



الشكل (٨,١). مسجل إزاحة.

مثال (٨,١,١)

يتكون مسجل الإزاحة في الشكل (٨,١) من أربعة مسجلات X_0, X_1, X_2, X_3 كل منها يحتوي على إحداثيات ثنائية. وكما هو مبين من الاتجاهات يتكون المخرج عند كل تكّة ساعة بجمع محتويات المسجلات الثلاثة X_0, X_1, X_3. لنفرض أن محتويات المسجلات X_0, X_1, X_2, X_3 هي 1,1,0,1 على التوالي. إذا كان المدخل التالي هو الإحداثي 0 فعند تكّة الساعة التالية، تتم إزاحة المدخل إلى المسجل X_0 وفي الوقت نفسه تتم إزاحة محتوى كل من المسجلات إلى المسجل الذي يليه. ولذا تكون المحتويات الجديدة للمسجلات X_0, X_1, X_2, X_3 هي 0,1,1,0 على التوالي ويكون المخرج هو $X_0 + X_1 + X_3 = 0 + 1 + 0 = 1$. ▲

لنفرض أن $a_0, a_1, a_2, \cdots$ هي متتالية مدخلات. عندئذ، يمكن استخدام جدول لمعرفة كل من المدخل، المخرج، محتويات المسجلات عند كل تكّة ساعة.

مثال (٨,١,٢)

لنفرض أن محتويات المسجلات الأربعة في مسجل إزاحة مراحل عددها 4 المبين في الشكل (٨,١) هي في البداية (0,0,0,0) وأن المدخلات $a_0, a_1, a_2, \cdots, a_6$ هي 1010000. الجدول التالي يلخص لنا محتويات المسجلات والمخرجات:

الزمن	المدخل	$X_0X_1X_2X_3$	المخرج $= X_0 + X_1 + X_3$
-1	—	0000	—
0	1	1000	1
1	0	0100	1
2	1	1010	1
3	0	0101	0
4	0	0010	0
5	0	0001	1
6	0	0000	0

ولهذا يكون مخرج مسجل الإزاحة هو 1110010 عندما يكون المدخل 1010000 ومحتويات المسجلات في البداية هي 0000. ▲

بصورة عامة، مسجل إزاحة مراحل عددها s هو مسجل إزاحة يحتوي على عدد s من المسجلات. مخرج مسجل إزاحة مراحل عددها s هو تركيب خطي لمحتويات المسجلات ويمكن وصفه باستخدام معاملات $g_0, g_1, \cdots, g_{s-1}$ حيث $g_i \epsilon K = \{0,1\}$. أي أن:

$$c_t = g_0 X_0(t) + g_1 X_1(t) + \cdots + g_{s-1} X_{s-1}(t)$$

حيث c_t هو المخرج عند الزمن t و $X_i(t)$ هو قيمة محتوى المسجل X_i عند الزمن t.

من الممكن استخدام كثيرات الحدود لوصف عمل هذه الأدوات، فإذا كانت $g_0, g_1, \cdots, g_{s-1}$ هي معاملات مسجل إزاحة مراحل عددها s فتكون كثيرة الحدود المقابلة لهذا المسجل هي:

$$.g(x) = g_0 + g_1 x + \cdots + g_{s-1} x^{s-1}$$

تُسمى كثيرة الحدود هذه بكثيرة الحدود المولّدة لمسجل الإزاحة. على سبيل المثال، $g(x) = 1 + x + x^3$ هي كثيرة حدود مولّدة لمسجل إزاحة مراحل عددها 4 المبين في الشكل (٨,١).

إذا كانت $a(x)$ كثيرة حدود المقابلة لمتتالية المدخل، $c(x)$ هي كثيرة الحدود المقابلة لمتتالية المخرج وكانت $g(x)$ هي كثيرة حدود مسجل الإزاحة فسنرى لاحقاً أن:

$$.c(x) = a(x)g(x)$$

مثال (٨,١,٣)

كثيرة حدود مسجل الإزاحة المبين في الشكل (٨,١) هي $g(x) = 1 + x + x^3$. كثيرة الحدود المقابلة لمتتالية المدخل 1010000 هي $a(x) = 1 + x^2$. إذا افترضنا بداية أن محتويات المسجلات الأربعة هي 0000 فنرى استناداً إلى المثال (٨,١,٢) أن متتالية المخرج هي 1110010 وكثيرة حدودها المقابلة هي $c(x) = 1 + x + x^2 + x^5$. وبهذا نرى أن:

$$\begin{aligned} a(x)g(x) &= (1 + x^2)(1 + x + x^2) \\ &= 1 + x + x^2 + x^5 \\ &= c(x) \end{aligned}$$

▲

مثال (٨,١,٤)

لنفرض أن $g(x) = 1 + x + x^3$ هي كثيرة الحدود المقابلة لمسجل الإزاحة المقدم في الشكل (٨,١). الجدول التالي يُبيّن متتالية المخرجات عندما تكون متتالية المدخلات هي $a_0, a_1, a_2, a_3, 0,0,0$.

الزمن	المدخل	X_0	X_1	X_2	X_3	المخرج $= X_0 + X_1 + X_3$
-1	—	0	0	0	0	—
0	a_0	a_0	0	0	0	a_0
1	a_1	a_1	a_0	0	0	$a_1 + a_0$
2	a_2	a_2	a_1	a_0	0	$a_2 + a_1$
3	a_3	a_3	a_2	a_1	a_0	$a_3 + a_2 + a_0$
4	0	0	a_3	a_2	a_1	$a_3 + a_1$
5	0	0	0	a_3	a_2	a_2
6	0	0	0	0	a_3	a_3

من الواضح أن:

$$\begin{aligned}
a(x)g(x) &= (a_0 + a_1x + a_2x^2 + a_3x^3)(1 + x + x^3) \\
&= a_0 + (a_1 + a_0)x + (a_2 + a_1)x^2 + (a_3 + a_2 + a_0)x^3 \\
&\quad +(a_3 + a_1)(x^4 + a_2x^5 + a_3x^6) \\
&= c(x)
\end{aligned}$$

معاملات $c(x)$ تقابل متتالية المخرجات لهذا المسجل. ▲

لتكن $g(x)$ كثيرة حدود شفرة خطيّة دورية من الدرجة $n - k$. من الممكن تصميم مسجل إزاحة مراحل عددها $n - k + 1$ كثيرة حدوده المولّدة هي $g(x)$ لغرض تشفير كثيرات حدود المعلومات $a(x)$ باستخدام كثيرات الحدود.

تمارين

(٨,١,٥) ارسم مخططاً لمسجل الإزاحة المقابل لكثيرة الحدود المولّدة $g(x)$ حيث:

(أ) $g(x) = 1 + x$ (ب) $g(x) = 1 + x^2$

(ج) $g(x) = 1 + x^2 + x^3$ (د) $g(x) = 1 + x^3 + x^4$.

(**٨,١,٦**) استخدم مسجل الإزاحة المنشأ في التمرين (**٨,١,٥**) لحساب $c(x) = a(x)g(x)$.

احسب $a(x)g(x)$ مباشرة ثم قارن الإجابتين :

(أ) $a(x) = 1 + x$ ، $g(x) = 1 + x^2$.

(ب) $a(x) = 1 + x^3 + x^6$ ، $g(x) = 1 + x^3 + x^4$.

(ج) $a(x) = x + x^2$ ، $g(x) = 1 + x^2 + x^3$.

(د) $a(x) = x^2 + x^5 + x^6$ ، $g(x) = 1 + x^3 + x^4$.

(**٨,١,٧**) افرض أن $g(x) = 1 + x + x^3$ هي كثيرة الحدود المولّدة لمسجل الإزاحة المقدم في الشكل (**٨,١**). احسب متتالية المخرجات $c_0, c_1, c_2, \cdots$ لكل من متتالية المدخلات $a_0, a_1, a_2, \cdots$ المبينة فيما يلي بافتراض أن محتويات جميع المسجلات هي في البداية 0 :

(أ) $10101000\cdots$.

(ب) $0011000\cdots$.

(ج) $1010010000\cdots$.

مبرهنة (٨,١,٨)

لتكن $g(x) = g_0 + g_1x + \cdots + g_{l-1}x^{l-1}$ كثيرة حدود مولّدة لمسجل إزاحة ولتكن $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ كثيرة الحدود المقابلة لمتتالية المخرجات $c_0, c_1, \cdots$. عندئذ ، $c(x) = a(x)g(x)$.

البرهان

لاحظ أولاً أنه إذا كان $c(x) = a(x)g(x)$ فإن :

$$c_t = \begin{cases} g_0a_t + g_1a_{t-1} + \cdots + a_0g_t & , t \le l-1 \\ g_0a_t + g_1a_{t-1} + \cdots + a_{t-l+1}g_{l-1} & , t > l-1 \end{cases}.$$

حيث افترضنا أن $a_t = 0$ عندما يكون $t > k - 1 = deg(a(x))$.

لنفرض الآن أن $g(x)$ هي كثيرة الحدود المولّدة لمسجل إزاحة. عندئذ، المخرج عند الزمن t هو تركيب خطي للمقادير $X_i(t)$:

$$c_t = g_0X_0(t) + g_1X_1(t) + \cdots + g_{l-1}X_{l-1}(t).$$

عند الزمن $t = 0$ يكون:

$$X_0(0) = a_0\ , X_1(0) = \cdots = X_{l-1}(0) = 0.$$

ومن ثم فإن $c_0 = g_0a_0$.

عند الزمن t حيث $t \leq l - 1$ يكون:

$$X_0(t) = a_t\ , X_1(t) = a_{t-1}, \cdots , X_t(t) = a_0.$$

ومحتويات بقية المسجلات أصفار. إذن،

$$c_t = g_0a_t + g_1a_{t-1} + \cdots + g_ta_0.$$

وأخيراً عند الزمن t حيث $t > l - 1$ يكون:

$$X_0(t) = a_t\ , X_1(t) = a_{t-1}, \cdots , X_{l-1}(t) = a_{t-l+1}.$$

وبهذا نرى أن:

$$c_t = g_0a_t + g_1a_{t-1} + \cdots + g_{l-1}a_{t-l+1}.$$

فعليه نخلص إلى أن $c(x) = a(x)g(x)$. ■

من الممكن تنفيذ ضرب كثيرات الحدود (ومن ثم استخدام كثيرات الحدود في تشفير الشفرات الدورية) باستخدام مسجلات الإزاحة على النحو التالي: كثيرة الحدود $g(x)$ المولّدة لمسجل الإزاحة هي كثيرة الحدود المولّدة للشفرة الخطيّة الدورية. من الممكن إجراء بعض التعديلات على مسجلات الإزاحة لنحصل على مسجلات إزاحة نستطيع استخدامها لتنفيذ قسمة كثيرات الحدود حيث تستخدم هذه في فك تشفير الشفرات الخطيّة الدورية. تُسمى الأداة التي تستخدم لتنفيذ قسمة كثيرات الحدود (ومن ثم فك تشفير الشفرات الخطيّة الدورية)، **مسجلات إزاحة ذات تغذية إرجاعية (Feedback Shift Registers)** أو اختصاراً FSR وهي عبارة عن مسجلات إزاحة تسمح

بإرجاع المخرجات إلى المسجلات. (يمكن للقارئ المهتم فقط بشفرات التلاف أن يتجاهل ما تبقى من هذا البند).

تذكّر أنه إذا كانت H مصفوفة اختبار نوعية لشفرة دورية كثيرة حدودها المولّدة هي $g(x)$ فإن الصف i من المصفوفة H هو $r_i \leftrightarrow r_i(x)$ حيث $r_i(x) \equiv x^i(mod\ g(x))$. وعلى وجه الخصوص $r_i(x) \equiv xr_{i-1}(x)(mod\ g(x))$.

مثال (٨,١,٩)

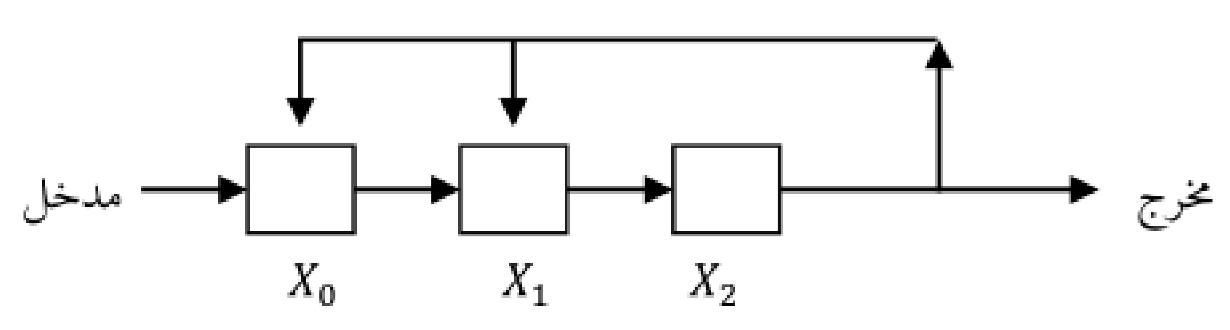
لتكن $g(x) = 1 + x + x^3$ كثيرة الحدود المولّدة. عندئذ، نرى في مصفوفة اختبار النوعية أن:

$$r_3 = 110 \leftrightarrow 1 + x \equiv x^3(mod\ g(x)).$$

$$r_4 = 011 \leftrightarrow x + x^2 \equiv x^4(mod\ g(x)).$$

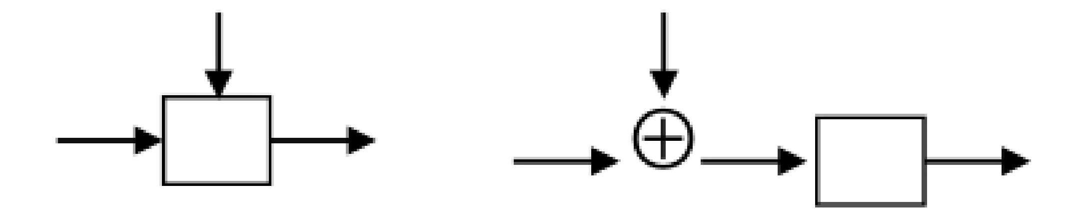
ولكن $r_5 \leftrightarrow x^2 + x^3(mod\ g(x))$ أو $r_5 = 001 + 110$.

ينظر إلى المتجه 110 على أنه المتجه الارجاعي الذي يتم جمعه ارجاعياً إلى المسجلات عندما يكون المخرج هو الإحداثي 1. مسجل الإزاحة ذو التغذية الإرجاعية المبين في الشكل (٨,٢) يوضح كيفية تنفيذ هذه العملية.



الشكل (٨,٢). مسجل إزاحة ذو تغذية إرجاعية.

إذا تم إدخال أكثر من إحداثي واحد إلى المسجل سنفترض أن محتوى المسجل هو المجموع الثنائي لهذه القيم. أي أن الشكلين التاليين يمثلان الوضع نفسه:



عند كل تكّة ساعة يتم إزاحة المدخل ومحتويات المسجلات ويتم أيضاً إضافة المخرج c_t إلى مسجلات مختارة. أي أن يتم إضافة المتجه الجديد $c_t(1,1,0)$ إلى محتويات المسجلات.

الزمن	المدخل	$X_0 + c_t$	$X_1 + c_t$	X_2	المخرج $= c_t$
-1	—	0	0	0	—
0	1	1	0	0	0
1	0	0	1	0	0
2	0	0	0	1	0
3	0	$0+1$	$0+1$	0	1
4	0	0	1	1	0
5	0	$0+1$	$0+1$	1	1
6	0	$0+1$	$1+1$	1	1
.7	0	1	0	0	1

▲

بصورة عامة، يوجد تقابل بين مسجل إزاحة مراحل عددها s ذي تغذية إرجاعية حيث $(g_0, g_1, \cdots, g_{s-1})$ هو متجه التغذية الإرجاعية وبين كثيرة الحدود من الدرجة s التالية:

$$g(x) = g_0 + g_1 x + \cdots + g_{s-1} x^{s-1} + x^s$$

محتويات المسجلات عند الزمن $t = deg(c(x))$ هي باقي خارج قسمة $c(x)$ على $g(x)$ ومتتالية المخرجات هي خارج القسمة $a(x)$. مع ملاحظة أن التغذية الإرجاعية لإحداثيات الكلمة المستقبلة تتم بترتيب عكسي للإحداثيات. لاحظ أن درجة كثيرة الحدود المقابلة لـ FSR تساوي s بينما درجة كثيرة الحدود المقابلة لمسجل إزاحة تساوي $s - 1$ ومع ذلك فعدد المسجلات في كلتا الحالتين يساوي s.

مثال (٨,١,١٠)

لتكن $x + x^2 + x^4$ هي كثيرة الحدود المستقبلة وأنها تقابل الكلمة 0110100. إذا كانت $g(x) = 1 + x + x^3$ فإن FSR المقابل لها هو المبين في الشكل (**٨,٢**).

الزمن	المدخل	X_0	X_1	X_2	المخرج
-1	—	0	0	0	—
0	1	1	0	0	0
1	0	0	1	0	0
2	1	1	0	1	0
3	1	$1+1$	$1+1$	0	1
4	0	0	0	0	0

باقي القسمة هو 000 وخارج القسمة هو $x \leftrightarrow 0100000$ ويقابل متتالية المخرجات بترتيب عكسي للإحداثيات. ▲

بصورة عامة، محتويات المسجلات عند الزمن $t = n$ هو الباقي $c(x)(mod\ g(x))$ حيث $c(x)$ تقابل متتالية المدخلات.

مبرهنة (٨,١,١١)

تغذية $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ إلى مسجل FSR الذي يقابل $g(x) = g_0 + g_1x + \cdots + 1x^s$ بترتيب عكسي للإحداثيات (أي $(c_{n-1}, c_{n-2}, \cdots, c_0$ تكافئ قسمة $c(x)$ على $g(x)$. المخرج بعد n تكّة ساعة هو خارج القسمة (بترتيب عكسي للمعاملات) ومحتويات المسجلات هي باقي القسمة (بترتيب عكسي للمعاملات).

البرهان

بما أن مخرج مجموع متتاليتي مدخلات هو مجموع متتاليتي المخرجات المقابلة فيكفي أن نتحقق من صواب المبرهنة للحالة $c(x) = x^l$. ولكن في هذه الحالة يكون من الواضح أن FSR يقابل الخوارزمية المقدمة سابقاً (انظر المثال (٤,٣,٧)) لحساب $(x^l(mod\ g(x))$. وبهذا فمحتويات المسجلات هي الباقي. كما أنه ليس بالأمر الصعب اثبات أن المخرج هو خارج قسمة $c(x)$ على $g(x)$. ■

تمارين

(**٨,١,١٢**) ليكن FSR هو المبيّن في الشكل (**٨,٢**) حيث تحتوي المسجلات بداية على أصفار. جد متتالية المخرجات لكل من الكلمات المستقبلة التالية. بيّن وضع المسجلات في النهاية وخارج القسمة إذا كان الباقي يساوي صفراً:

(أ) 0011010 (ب) 1010110 (ج) 0010001.

(**٨,١,١٣**) لتكن $g(x) = 1 + x + x^3$. احسب كثيرة حدود التناذر لكل من الكلمات المستقبلة في التمرين (**٨,١,١٢**). قارن كثيرة حدود التناذر مع كثيرة الحدود المقابلة للوضع النهائي للمسجلات التي وجدت في التمرين (**٨,١,١٢**).

(**٨,١,١٤**) لكل من كثيرات الحدود المولّدة أنشئ FSR. احسب متتالية المخرجات ثم جد الوضع النهائي للمسجلات لمتتالية المدخلات $c(x)$.

(أ) $g(x) = 1 + x^2 + x^3$ ، $c = 0010110$.

(ب) $g(x) = 1 + x + x^2$ ، $c = 111$.

(ج) $g(x) = 1 + x + x^4$ ، $c = 010000000100000$.

(**٨,٢**) تشفير شفرات التلاف

Encoding Convolutional Codes

شفرات التلاف هي شفرات عملية جداً وهي تستخدم إضافة إلى شفرات ريد وسولومن من قبل NASA و ESA للوثوق من صحة الاتصالات أثناء القيام بالرحلات الفضائية.

تُشفّر كل من الرسائل أولاً باستخدام شفرة ريد وسولومن ومن ثم تستخدم شفرة التلاف لتشفير الرسالة الناتجة عن ذلك. ندرس في البنود القادمة عملية تشفير وفك التشفير باستخدام شفرات التلاف ونناقش بعض المسائل التي تنشأ عن هذه الشفرات ونبدأ بالتعريف التالي:

شفرة التلاف (الثنائية) من النوع $(n, k = 1, m)$ وذات كثيرات الحدود المولّدة $g_1(x), \cdots, g_n(x)$ حيث $g_i(x) = g_{i,0} + g_{i,1}x + \cdots + g_{i,m}x^m$ ، $g_i \epsilon K[x]$ هي الشفرة المكوّنة من كلمات الشفرة $c(x) = (c_1(x), c_2(x), \cdots, c_n(x))$ حيث $c_i(x) = m(x)g_i(x)$ و $m(x) = m_0 + m_1x + m_2x^2 + \cdots \epsilon K[x]$. (سنكتب بالتفصيل عن العدد k لاحقاً حيث اعتبرنا لغرض السهولة أن قيمته تساوي 1 في هذا التعريف). لاحظ أن $m(x)$ هي الرسالة التي يتم تشفيرها إلى $c(x)$. لنفرض أن كلاً من $c(x)$ و $c'(x)$ كلمة شفرة. عندئذ ،

$$\begin{aligned} c(x) + c'(x) &= \big(c_1(x), \cdots, c_n(x)\big) + (c'_1(x), \cdots, c'_n(x)) \\ &= \big(m(x)g_1(x), \cdots, m(x)g_n(x)\big) + \big(m'(x)g_1(x), \cdots, m'(x)g_n(x)\big) \\ &= \big(\big(m(x) + m'(x)\big)g_1(x), \cdots, \big(m(x) + m'(x)\big)g_n(x)\big) \end{aligned}$$

وهذا ما هو إلا كلمة الشفرة المقابلة للرسالة $m(x) + m'(x)$. إذن، شفرة التلاف هي شفرة خطيّة.

وجه الاختلاف بين شفرات التلاف والشفرات التي درسناها سابقاً هو أن طول الشفرات وطول الرسائل غير منته في شفرات التلاف.

مثال (٨,٢,١)

لتكن C_1 شفرة تلاف من النوع $(2,1,3)$ حيث $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$. سنستخدم C_1 لتشفير الرسالتين التاليتين :

(أ) يتم تشفير الرسالة $m(x) = 1 + x^2$ إلى :

$$\begin{aligned} c(x) &= \big((1 + x^2)g_1(x), (1 + x^2)g_2(x)\big) \\ &= (1 + x + x^2 + x^5\, , 1 + x^3 + x^4 + x^5) \\ &\leftrightarrow (11100100 \cdots, 10011100 \cdots) \end{aligned}$$

(ب) يتم تشفير الرسالة $m(x) = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i$ إلى :

$$c(x) = (1 + x^3 + x^4 + x^5 + \cdots, 1 + x + x^3 + x^4 + x^5 + \cdots)$$

$$= \left(1 + \sum_{i=3}^{\infty} x^i , 1 + x + \sum_{i=3}^{\infty} x^i\right)$$

$$\leftrightarrow (100111\cdots,110111\cdots) \quad ▲$$

تمارين

(**٨,٢,٢**) شفّر الرسائل التالية باستخدام شفرة تلاف من النوع (3,1,3) حيث كثيرات الحـدود المولّـدة هـي $g_1(x) = 1 + x + x^3$ ، $g_2(x) = 1 + x + x^2 + x^3$ ، $g_3(x) = 1 + x^2 + x^3$.

(أ) $m(x) = 1 + x^3$ (ب) $m(x) = 1 + x + x^3$

(ج) $m(x) = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$.

(**٨,٢,٣**) شفّر الرسائل التالية باستخدام شفرة تلاف من النوع (2,1,4) حيث كثيرتي الحدود المولّدة هي $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

(أ) $m(x) = 1 + x + x^2$ (ب) $m(x) = 1 + x + x^3$

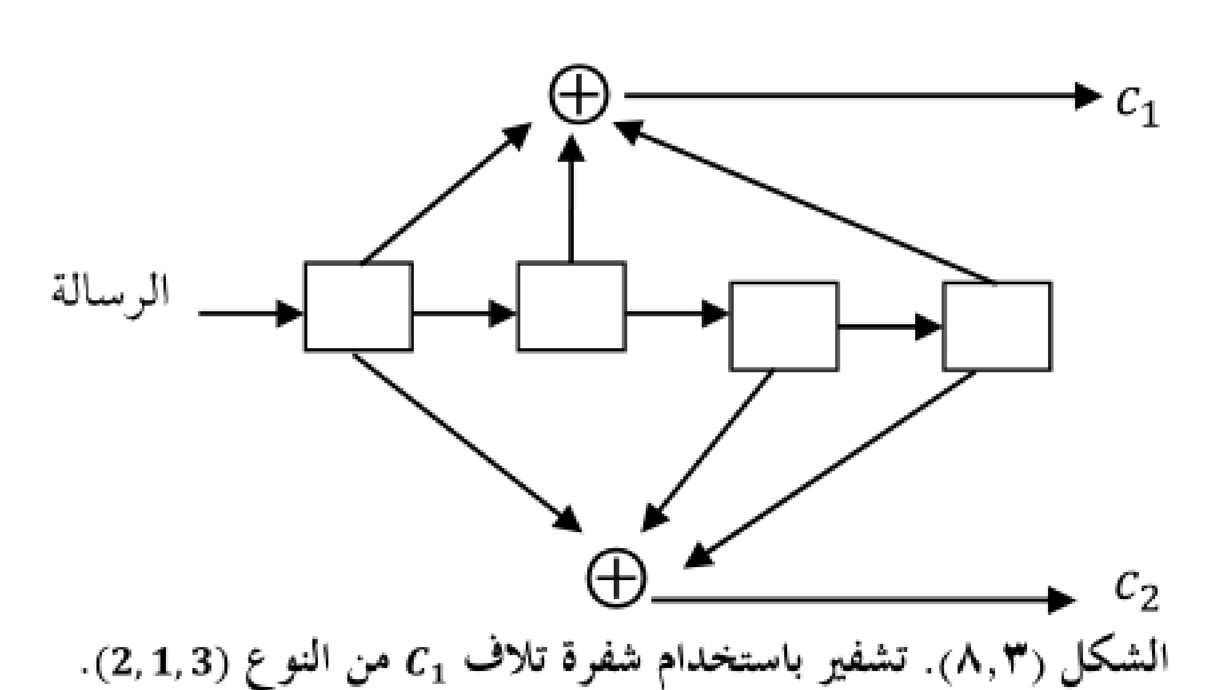
(ج) $m(x) = 1 + x^2 + x^4 + \cdots = \sum_{i=0}^{\infty} x^{2i}$.

استناداً إلى المبرهنة (**٨,١,٨**) نرى إمكانية وصف شفرات التلاف بدلالة مسجلات الإزاحة على النحو التالي:

$c_i(x)$ هي مخرج مسجل الإزاحة المولّد بكثيرة الحدود $g_i(x)$ عندما يكون المدخل هو $m(x)$.

مثال (٨,٢,٤)

يمكن وصف شفرة التلاف C_1 المقدمة في المثال (**٨,٢,١**) بدلالة مسجل إزاحة كثيرتي حدوده المولّدة وهما $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$ كما هو مبيّن في الشكل (**٨,٣**).



الشكل (٨,٣). تشفير باستخدام شفرة تلاف C_1 من النوع $(2,1,3)$.

باستخدام هذا الوصف، إذا كانت الرسالة المراد تشفيرها هي $m(x) = 1 + x^2 \leftrightarrow 10100\cdots$ فإن $c_1 = 11100100\cdots$ وهذا يتفق مع الحسابات التي أُجريت في المثال (٨,٢,١). وبالمثل يمكن رؤية أن c_2 هي $10011100\cdots$. ▲

من الممكن تحويل $c(x)$ إلى إحداثيات كلمة واحدة عوضاً عن إحداثيات n من الكلمات، وذلك بالتوريق البيني لكثيرات الحدود $c_1(x), c_2(x), \cdots, c_n(x)$. في ما تبقى من هذا الفصل سنعتبر أن $c(x)$ مورّقة بينياً وبهذا يتكون المخرج من معاملات x^0 في كثيرات الحدود $c_1(x), \cdots, c_n(x)$ متبوعة بمعاملات $x, x^2, \cdots$. وعند عرض $c \leftrightarrow c(x)$ بهذا الشكل للتوريق البيني نقوم بضم الإحداثيات التي عددها n والتي هي معاملات x^i ، $i \geq 0$ بعضها مع بعض.

مثال (٨,٢,٥)

التوريق البيني لتمثيل $c(x)$ المقدمة في المثال (٨,٢,١) (أ) هو:

$$c = 11\ 10\ 10\ 01\ 01\ 11\ 00\ 00\ \cdots$$

والتوريق البيني لتمثيل $c(x)$ المقدمة في المثال (٨,٢,١) (ب) هو:

$$.c = 11\ 01\ 00\ 11\ 11\ 11\ \cdots$$ ▲

تمرين

(**٨,٢,٦**) أنشئ مسجل إزاحة مناسب للتشفير لكل من شفرتي التلاف المقدمتين في التمرينين (**٨,٢,٢**) و (**٨,٢,٣**). ثم استخدم مسجل الإزاحة لتشفير الرسائل المقدمة في التمرينين. جد التوريق البيني لكل من كلمات الشفرة.

إذا تم تشفير شفرة تلاف ثنائية من النوع $(n,1,m)$ باستخدام مسجلات الإزاحة فنرى أن إزاحة إحداثي واحد من إحداثيات الرسالة إلى مسجل الإزاحة ينتج عنه عدد n من إحداثيات الشفرة بواقع إحداثي واحد لكل من $c_1(x),\cdots,c_n(x)$. وبهذا يكون معدل المعلومات لمثل شفرة التلاف هذه هو $\frac{1}{n}$ (تذكر أن معدل معلومات شفرة يقيس جزء المعلومات التي يحملها كل إحداثي من إحداثيات كلمة الشفرة). ولذا، يكون من المناسب إنشاء شفرات تلاف معدل معلوماتها مختلف عن $\frac{1}{n}$، وعلى وجه الخصوص شفرات تلاف معدل معلوماتها أكبر من $\frac{1}{2}$.

إن الطريقة الواضحة لإنجاز ذلك تكون بتحريك أكثر من إحداثي واحد (وليكن عدد k من الإحداثيات) من إحداثيات الرسالة إلى مسجل الإزاحة قبل القيام بحساب الإحداثيات التالية لكلمات الشفرة، وبهذا نحصل على شفرة معدل معلوماتها يساوي $\frac{k}{n}$. وهذا في الحقيقة هو دور العدد k في تعريف شفرة التلاف من النوع (n,k,m). لاحظ أنه لو اتبعنا ذلك لوجدنا أن كل إحداثي من إحداثيات الرسالة سيظهر في المسجلات $X_i, X_{i+k}, X_{i+2k},\cdots$ حيث i عدد يحقق $0 \le i < k$. ولذا عوضاً عن تحريك k من إحداثيات الرسالة في الوقت نفسه إلى مسجل الإزاحة فمن الممكن اتباع اسلوب مكافئ وهو تقسيم مسجل الإزاحة إلى k من مسجلات الإزاحة:

$$X_0, X_k, X_{2k},\cdots, X_1, X_{k+1}, X_{2k+1},\cdots,\cdots$$

وفي المقابل تكون الرسالة قد قسمت إلى k من الكلمات كل منها تدخل إلى واحد من مسجلات الإزاحة التي عددها k. المشكلة الوحيدة التي تنشأ عن ذلك هي أن محتويات

المسجلات في مسجلات إزاحة مختلفة يتم ضم بعضها مع بعض لتشكل مولّداً واحداً. وهذه هي الطريقة المتبعة عند التطبيق العملي لعملية التشفير، ونوضّح ذلك بالمثال التالي.

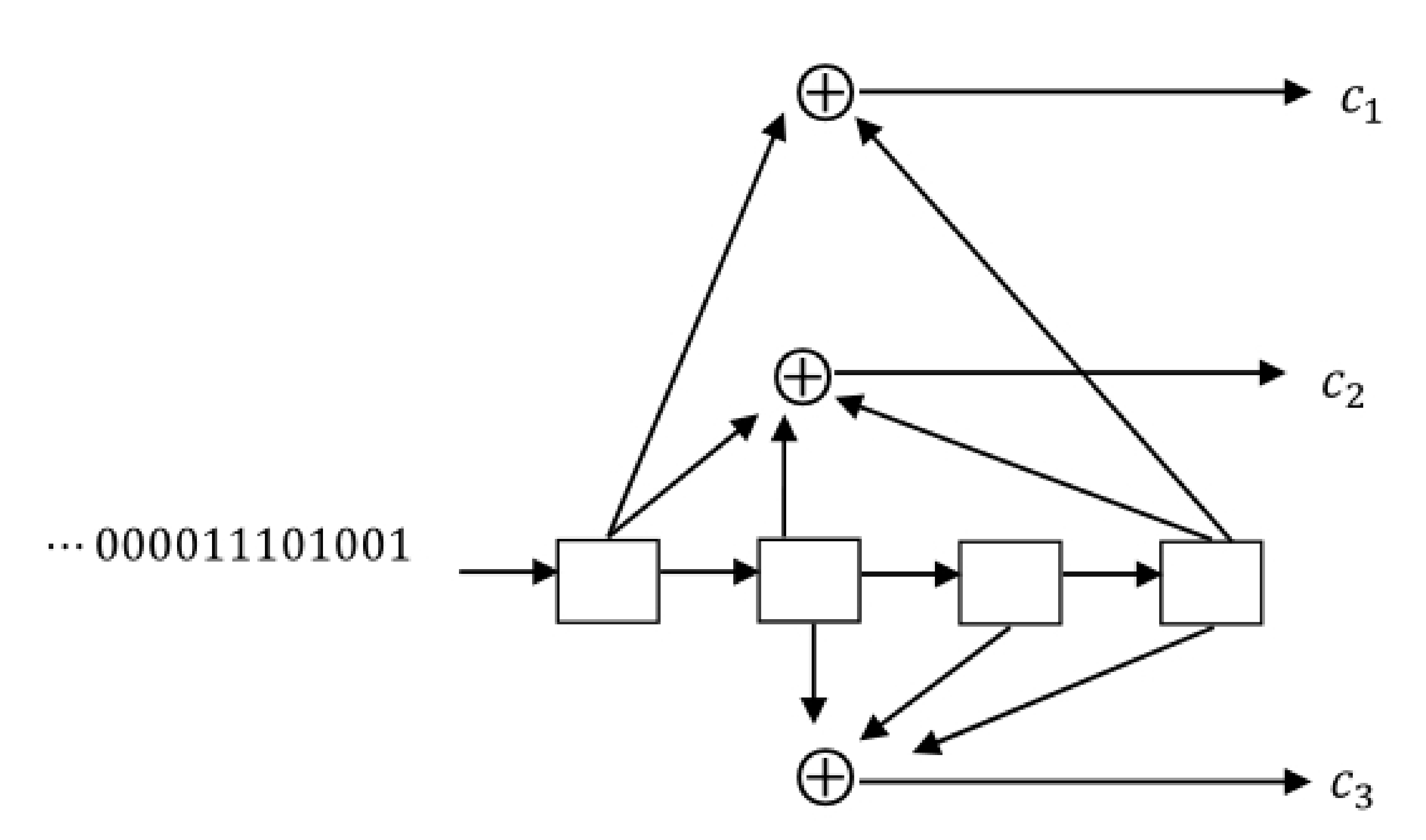
مثال (٨,٢,٧)

استخدم شفرة التلاف C من النوع (3,2,3) وذوات المولّدات $g_1(x) = 1 + x^3$ ، $g_2(x) = 1 + x + x^3$ ، $g_3(x) = x + x^2 + x^3$ لتشفير الرسالة :

$.m = 100101110000 \cdots$

الحل

التفسير الأول للقيمة $k = 2$ هو تشفير الرسالة m باستخدام مسجل إزاحة واحد مبيّن في الشكل (٨,٤) ومن ثم إزاحة إحداثيين $(k = 2)$ من إحداثيات الرسالة إلى مسجل الإزاحة مع كل تكّة ساعة. الجدول التالي يلخص لنا محتويات المسجلات والمخرجات :



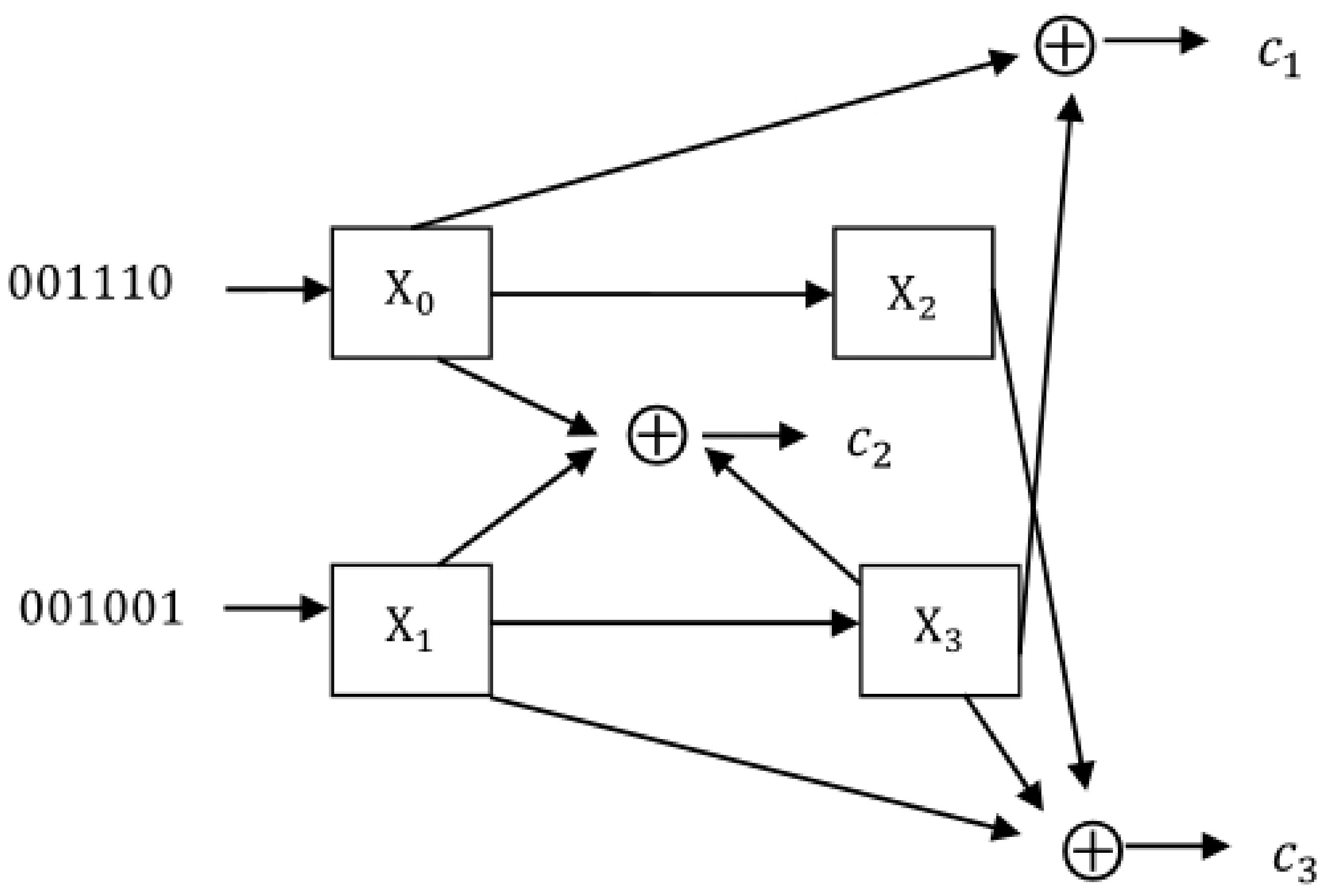
الشكل (٨,٤). تشفير باستخدام شفرة تلاف من النوع (3,2,3).

الزمن	المدخل	$X_0X_1X_2X_3$	المخرج c_1 c_2 c_3
−1	—	0000	—
0	01	0100	011
1	10	1001	001
2	10	1010	111
3	11	1110	100
4	00	0011	110
5	00	0000	000

وبهذا يكون تشفير الرسالة m (بعد التوريق البيني) هو:

$$.c = 011\ \ 001\ \ 111\ \ 100\ \ 110\ \ 000\ \ \cdots$$

أما التفسير الثاني للعدد $k = 2$ فهو ملاحظة أن الإحداثيات الأول، الثالث، الخامس، ⋯ من الرسالة يتم إدخالها إلى مسجل الإزاحة فقط عند ظهورها في X_0 و X_2 وأن الإحداثيات الثاني، الرابع، السادس، ⋯ من الرسالة يتم إدخالها إلى مسجل الإزاحة فقط عند ظهورها في X_1 و X_3. وبهذا نستطيع تقسيم الرسالة والمسجلات إلى جزأين $(k = 2)$ كما هو مبيّن في الشكل (٨,٥). ▲



الشكل (٨,٥). تشفير باستخدام شفرة تلاف من النوع (3,2,3).

تمرين

(**٨,٢,٨**) شفّر الرسائل التالية باستخدام شفرة تلاف من النوع (3,2,4) حيث مولّداتها هي $g_1(x) = 1 + x^3$ ، $g_2(x) = x + x^4$ ، $g_3(x) = 1 + x + x^2 + x^3 + x^4$.

استخدم تقنيتي التشفير المبينتين في هذا البند.

(أ) $m(x) = 1 + x + x^3 + x^4 + x^5$.

(ب) $m(x) = 1 + x^3 + x^5 + x^7 + x^8$.

(ج) $m(x) = 1 + x + x^2 + x^3$.

ناقش في ما تبقى من هذا الفصل شفرات التلاف الثنائية من النوع $(2,1,m)$ ذات معدل المعلومات $r = \frac{1}{2}$. يمكن تعميم جميع النتائج والتقنية المستخدمة لشفرات التلاف من النوع (n,k,m) حيث الأفكار الرئيسة مشابهة للأفكار المقدمة في الشفرة الأسهل من النوع $(2,1,m)$. القارئ المهتم بدراسة شفرات التلاف عندما يكون $k > 1$ يستطيع الرجوع إلى التمارين لرؤية كيفية تعميم المادة المقدمة للشفرات في الحالة $k = 1$ إلى شفرات تلاف حيث $k > 1$.

من المناسب أن نذكر هنا أن **مسّاح المريخ الشامل** (**Mars Global Surveyor**) الذي أطلق من قبل NASA يستخدم شفرة تلاف حيث $r = \frac{1}{2}$ و $m = 7$ أثناء إرساله معلومات من المريخ إلى الأرض وأن **مستكشف المريخ** (**Mars Pathfinder**) يستطيع اختيار شفرة تلاف حيث $(r,m) = (\frac{1}{2}, 7)$ أو $(r,m) = (\frac{1}{6}, 15)$. تستطيع مشاهدة الصور التي التقطت من قبل بعثات NASA على الموقع http://www.msss.com.

أخيراً، توجد طريقة أخرى للتشفير باستخدام شفرات التلاف. تذكّر أنه من الممكن تشفير شفرة تلاف من النوع $(2,1,m)$ باستخدام مسجل إزاحة مكوّن من $m + 1$ مسجلاً. عند كل تكّة ساعة، تُسمى محتويات المسجلات الـ m الأولى، مرحلة **مسجل الإزاحة** (**State of the Shift Register**). المرحلة صفر هي المرحلة التي تكون

فيها محتويات المسجلات الـ m الأولى أصفاراً. إذا كان مسجل الإزاحة في المرحلة $s_0, s_1, \cdots, s_{m-1}$ فعند تكّة الساعة التالية إما أن ينتقل مسجل الإزاحة إلى المرحلة $0, s_0, s_1, \cdots, s_{m-2}$ وإما إلى المرحلة $1, s_0, s_1, \cdots, s_{m-2}$ وهذا يعتمد على كون إحداثي الرسالة الذي تم إزاحته إلى المسجل X_0 هو 0 أو 1 على التوالي. أيضاً، إذا علمنا المرحلة الحالية $s_0, s_1, \cdots, s_{m-1}$ والمرحلة السابقة $s_1, \cdots, s_m$ فنستطيع معرفة المحتويات الحالية لجميع المسجلات ومن ثم نستطيع معرفة المخرج الحالي. تمثل هذه المعلومات في العادة بيانياً: مخطط المراحل لشفرة تلاف من النوع $(2,1,m)$ هو **رسم موجّه (Directed Graph)** رؤوسه (أو مراحله) هي جميع الكلمات الثنائية ذات الطول m، ولكل مرحلة $s = s_1, s_2, \cdots, s_m$ يوجد ضلع موجّه من s إلى المرحلة$0, s_1, s_2, \cdots, s_{m-1}$ مُعلّماً بالمخرج عندما تحتوي المسجلات $X_0, X_1, \cdots, X_m$ على $1, s_1, \cdots, s_m$ على التوالي.

من الممكن أيضاً تمثيل مخطط المراحل لشفرة تلاف من النوع $(2,1,m)$ على شكل جدول: كل من صفوف الجدول يُبيّن المرحلة الحالية (أي محتويات $X_0, X_1, \cdots, X_{m-1}$) والمخرج المقابل لها وهذا بالطبع يعتمد على كون $X_m = 0$ أو $X_m = 1$.

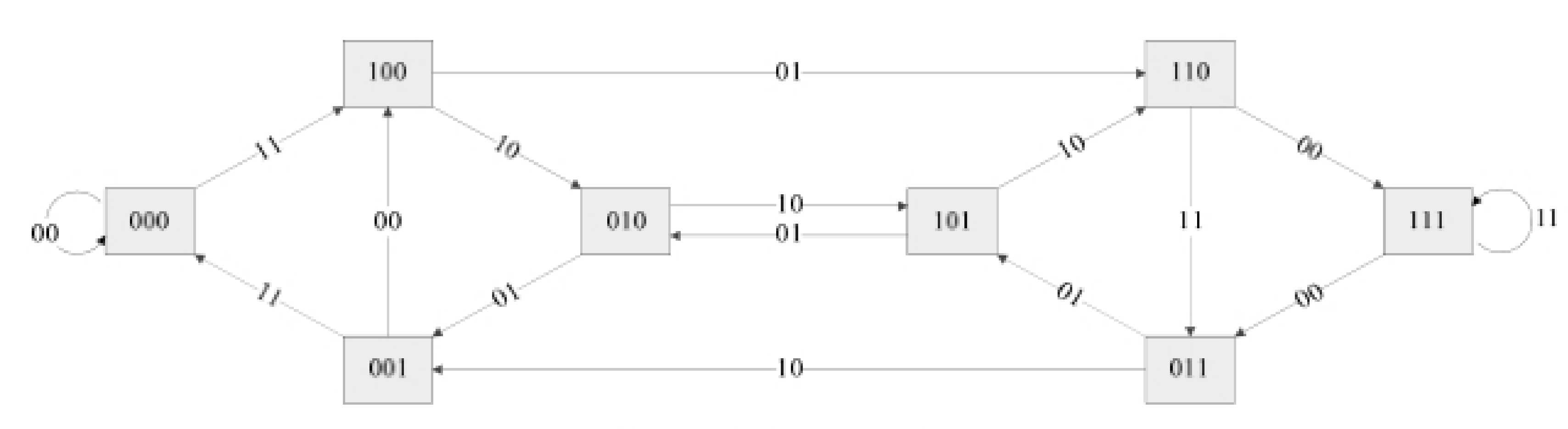
مثال (٨,٢,٩)

لنفرض أن C_1 شفرة تلاف من النوع $(2,1,3)$ مولداها $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$ (انظر المثالين (٨,٢,١) و (**٨,٢,٤**)). المراحل هي جميع الكلمات الثنائية ذات الطول $m = 3$:

$$.000,100,010,001,110,101,011,111$$

على سبيل المثال، يوجد ضلع موجّه من المرحلة $s = s_1 s_2 s_3 = 011$ إلى المرحلة $0 s_1 s_2 = 001$ وضلع موجّه من s إلى $1 s_1 s_2 = 101$. الضلع الموجّه من 011 إلى 001 يُعلَّم بالمخرج عندما يكون $X_0 X_1 X_2 X_3 = 0011$، بالتحديد 10 والضلع الموجّه من 011

إلى 101 يُعلَّم بالمخرج عندما يكون $X_0X_1X_2X_3 = 1011$ ، بالتحديد 01. وباكمال ذلك لجميع المراحل نحصل على مخطط المراحل (الرسم الموجّه) المبيّن في الشكل (٨,٦).



الشكل (٨,٦). مخطط المراحل للشفرة C_1.

يمكن أيضاً تمثيل مخطط المراحل في الجدول التالي:

المرحلة	المخرج	
$X_0X_1X_2$	$X_3 = 0$	$X_3 = 1$
000	00	11
100	11	00
010	10	01
110	01	10
001	01	10
101	10	01
011	11	00
111	00	11

تذكر أن محتويات كل مسجلة بداية هي 0 ومن ثم فمرحلة البداية لمسجل الإزاحة هي $X_0X_1 \cdots X_{m-1} = 00 \cdots 0$. عند إدخال كل إحداثي من إحداثيات الرسالة إلى مسجل الإزاحة يتحرك مسجل الإزاحة إلى مرحلة أخرى وينتج عن كل مولّد إحداثي شفرة مخرجة. إن هذا يقابل في مخطط المراحل الحركة من مرحلة إلى المرحلة المجاورة (باتجاه الضلع الموجّه) والمخرجات هي علامات الأضلاع الموجّهة. وبهذا تقابل كلمة شفرة

مساراً موجّهاً في مخطط المراحل يبدأ عند المرحلة 0 ويتحرك باتجاه الأضلاع الموجّهة إلى المراحل المجاورة. لاحظ أنه عند كل تكّة ساعة، إحداثي الرسالة الذي يتحرك إلى مسجل الإزاحة هي الإحداثي الأول من المرحلة في مخطط المراحل. أيضاً، يكون من السهل معرفة الرسالة المقابلة لأي كلمة شفرة. ▲

مثال (٨,٢,١٠)

بالرجوع إلى المثالين (**٨,٢,١**) و (**٨,٢,٩**)، تُقابل الرسالة:

$$m(x) = 1 + x^2 \leftrightarrow 10100 \cdots$$

المسار الذي يبدأ عند المرحلة 000 ومن ثم يتحرك إلى المراحل:

$$100,010,101,010,001,000,000, \cdots$$

على التوالي. علامات الأضلاع الموجّهة هذه هي:

$$11,10,10,01,01,01,11,00, \cdots$$

على التوالي، وهذه هي كلمة الشفرة التي تم تشفير الرسالة $m(x)$ لها (بعد التوريق البيني، انظر المثال (**٨,٢,٥**)). أيضاً، نستطيع وبسهولة الحصول على رسالة مقابلة لكلمة شفرة مُعطاة، فإذا كانت:

$$c = 00\ \ 11\ \ 01\ \ 11\ \ 01\ \ 01\ \ 01\ \ 11\ \ 00\ \ \cdots$$

فيكون المسار في مخطط المراحل الذي تنتج عنه الكلمة c هو المسار الذي يمر بالمراحل:

$$000,000,100,110,011,101,010,001,000,000, \cdots$$

(من المؤكد أن جميع كلمات الشفرة تبدأ عند المرحلة الصفرية 000). وبما أنه عند كل تكّة ساعة، يكون إحداثي الرسالة هي الإحداثي الأول في المرحلة التي يتحرك إليها المسجل، نرى أن الرسالة التي تقابل c هي التي نحصل عليها من الإحداثي الأول لكل مرحلة من مراحل المسار (عدا مرحلة البداية). أي أن:

$$m = 0\,1\,1\,0\,1\,0\,0\,0\,0 \cdots.$$ ▲

تمارين

(**٨,٢,١١**) (أ) جد مخطط المراحل ومثله على شكل جدول لشفرة التلاف من النوع (2,1,2) التي لها المولّدان $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$.

(ب) استخدم مخطط المراحل لتشفير كل من الرسالتين:

(i) $m(x) = 1 + x^2$

(ii) $m(x) = 1 + x + x^2$.

(ج) استخدم مخطط المراحل لإيجاد الرسالة التي تقابل كلاً من كلمتي الشفرة:

(i) $11\ 01\ 00\ 01\ 11\ 00\ \cdots$.

(ii) $00\ 11\ 10\ 01\ 01\ 10\ 00\ \cdots$.

(**٨,٢,١٢**) (أ) جد مخطط المراحل ومثله على شكل جدول لشفرة التلاف من النوع (2,1,3) التي لها المولّدان $g_1(x) = 1 + x + +x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$.

(ب) استخدم مخطط المراحل لتشفير الرسائل التالية:

(i) $m(x) = 1 + x^3$

(ii) $m(x) = 1 + x + x^3$

(iii) $m(x) = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$.

(ج) استخدم مخطط المراحل لإيجاد الرسالة التي تقابل كلاً من كلمتي الشفرة:

(i) $11\ 10\ 00\ 01\ 00\ 10\ 10\ \cdots$.

(ii) $00\ 11\ 01\ 10\ 01\ 10\ 00\ \cdots$.

(**٨,٢,١٣**) (أ) جد مخطط المراحل ومثله على شكل جدول لشفرة التلاف من النوع (2,1,4) التي لها المولّدان $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

(ب) استخدم مخطط المراحل لتشفير الرسائل التالية:

(i) $m(x) = 1 + x + x^2$

(ii) $m(x) = 1 + x + x^3$

(iii) $m(x) = 1 + x^2 + x^4 + \cdots = \sum_{i=0}^{\infty} x^{2i}$.

قارن إجاباتك مع إجابات التمرين (**٨,٢,٣**).

(**٨,٢,١٤**) إذا كان $1 \le k \le \frac{m}{2}$ فمن الممكن تعريف مخطط المراحل لشفرة تلاف من النوع (n,k,m) بصورة مشابهة للتعريف المقدم على النحو التالي:
المراحل هي جميع الكلمات الثنائية ذات الطول $m+1-k$ ولكل مرحلة $s = s_k, s_{k+1}, \cdots, s_m$ وكل كلمة ثنائية u من الطول k يوجد ضلع موجّه من المرحلة s إلى المرحلة $u, s_{k+1}, \cdots, s_{m-k}$ مُعَلَّم بالمخرج عندما تحتوي المسجلات $X_0, X_1 \cdots, X_m$ على $u, s_{k+1}, \cdots, s_{m-k}$. (عندما يكون $k > 1$) استخدمنا توصيف التشفير بإزاحة k إحداثياً من إحداثيات الرسالة إلى مسجل واحد من مسجلات الإزاحة عند كل تكّة ساعة). جد مخطط المراحل لشفرة التلاف من النوع (n,k,m) عندما تكون مولّداتها هي:

(أ) $g_1(x) = 1 + x + x^3$ ، $g_2(x) = 1 + x + x^2 + x^3$ ، $g_3(x) = 1 + x^2 + x^3$ حيث $k = 1$.

(ب) $g_1(x) = 1 + x^3$ ، $g_2(x) = 1 + x + x^3$ ، $g_3(x) = x + x^2 + x^3$ حيث $k = 2$.

(ج) $g_1(x) = 1 + x^3$ ، $g_2(x) = x + x^4$ ، $g_3(x) = 1 + x + x^2 + x^3 + x^4$ حيث $k = 2$.

(٨,٣) فك تشفير شفرات التلاف
Decoding Convolutional Codes

كلمات شفرات التلاف ذات طول غير منته، ولذا يكون من الطبيعي توقع اختلاف فك تشفيرها عن فك تشفير الشفرات الأخرى. ولتجنب مشكلات التخزين فعملية فك التشفير تبدأ قبل الانتهاء من استقبال جميع إحداثيات كلمة الشفرة ومن ثم فعلينا تحديد زمن الانتظار اللازم قبل البدء بفك التشفير. على سبيل المثال، لتكن C_1 هي شفرة التلاف من النوع (2,1,3) حيث مولّداها هما $g_1(x) = 1 + x + x^3$

و $g_2(x) = 1 + x^2 + x^3$ (مخطط المراحل لهذه الشفرة هو المخطط المبيّن في الشكل (٨,٦)). لنفرض أن الكلمة المستقبلة هي :

$$w(x) = 1 + x \leftrightarrow 11\ \ 00\ \ 00\ \ 00\ \ \cdots = w.$$

تذكر أن كلمات الشفرة تقابل مسارات موجّهة في مخطط المراحل تبدأ بالمرحلة 000 ، ولكن من الواضح عدم وجود مسار موجّه مخرجه w. ولهذا يتوجب علينا إيجاد أقرب كلمة شفرة للكلمة w. أي ايجاد مسار موجّه في مخطط المراحل يكون مخرجه قريباً من w. عند معرفتنا جميع إحداثيات w نرى أن المسار الموجّه الذي لا يغادر المرحلة 000 يقابل كلمة الشفرة $c_1 = 00\ \ 00\ \ 00\ \ \cdots$ التي تبعد مسافة مقدارها 2 عن الكلمة w. ومن السهل التحقق من أن أي مسار موجّه آخر يكون مخرجه كلمة تختلف عن الكلمة w بأكثر من إحداثيين. إذن ، c_1 هي كلمة الشفرة الأقرب ويكون فك تشفير w هو الرسالة $m = 000\cdots$.

لنفترض الآن أن سعة التخزين محدودة جداً بحيث يتوجب علينا فك تشفير إحداثي من إحداثيات الرسالة عند كل تكّة ساعة. عند التكّة الأولى نبدأ عند المرحلة 000 ونرى أن 11 إحداثيان من إحداثيات w. وبما أن الضلع الموجّه من 000 إلى 100 مُعَلَّم بالإحداثيين 11 فالخيار الأفضل لنا هو التحرك إلى المرحلة 100 وهو الخيار الذي مخرجه يتفق مع إحداثيات الكلمة المستقبلة w. إذن ، نقوم بفك تشفير الإحداثي الأول من الرسالة على أنه الإحداثي 1. عند التكّة الثانية نكون في المرحلة 100 ولدينا الإحداثيان 00 من الكلمة w ومن ثم نقع في المأزق التالي :

إما التحرك إلى المرحلة المجاورة 010 وإما المرحلة المجاورة 110 لنحصل على المخرج 10 أو 01 على التوالي وكلاهما يبعد مسافة 1 عن الإحداثيات المستقبلة. وبهذا يتوجب علينا أخذ قرار اعتباطي حيث اكتشفنا وقوع خطأ أثناء الإرسال لا نستطيع تصويبه. وإما أن يكون فك تشفير w هو $c_2 = 11\ \ 10\ \ \cdots$ أو $c_2' = 11\ \ 01\ \ \cdots$ حيث

الرسالة الأقرب هي $m = 1 * \cdots$ (العلامة * تعني أننا قمنا باتخاذ قرار اعتباطي عند اختيار فك تشفير الإحداثي ليكون 0 أو 1). لاحظ أن فك التشفير * يتوجب عليه أن يكون اختيار المرحلة التالية اعتباطياً أيضاً من بين المرحلتين المجاورتين للمرحلة الحالية.

ندرس الآن خياراً آخر وهو إمكانية تخزين معلومات تكتين قبل البدء بعملية فك التشفير. في هذه الحالة نبدأ بأخذ جميع المسارات من المرحلة الصفرية التي طول كل منها يساوي 2 ونقارن علامات أضلاعها مع أول تكّتين للكلمة w، بالتحديد مع 00 11 لنحصل على معلومات الشكل (٨,٧).

المسار	المخرج	المسافة من 00 11
000,000,000	00 00	2
000,000,100	00 11	4
000,100,010	11 10	1
000,100,110	11 01	1

الشكل (٨,٧). معلومات قرار فك التشفير الأول.

من هذه المعلومات نرى وجود مسارين هما الأقرب إلى 00 11 وهو الجزء المعروف من الكلمة w لحد الآن. وهذا لا يسبب أي مشكلة ؛ لأن المسارين يتفقان في أن الحركة الأولى يجب أن تكون إلى المرحلة 100. وهذان المساران يختلفان فقط في القرار الذي يجب علينا اتخاذه للتحرك من المرحلة 100 وهو قرار ليس علينا اتخاذه إلا بعد استقبال إحداثيات أخرى من w. إذن، يكون قرار فك التشفير في هذه الحالة هو التحرك إلى المرحلة 100 ويتم فك تشفير الإحداثي الأول من الرسالة على أنه الإحداثي 1. نستخدم الآن التكّتان الثانية والثالثة من معلومات w (أي 00 00) لاتخاذ قرار فك التشفير التالي. نقوم بايجاد المسافة بين 00 00 ومخرجات جميع المسارات من الطول 2 التي تبدأ عند المرحلة الحالية 100 كما هو مبين في الشكل (٨,٨).

المسار	المخرج	المسافة من 00 00
100,010,001	10 01	2
100,010,101	10 10	2
100,110,111	01 11	3
100,110,111	01 00	1

الشكل (٨,٨). معلومات قرار فك التشفير الثاني.

في هذه الحالة نرى وجود مسار هو وحيد هو الأقرب إلى الجزء المختار من w. هذا المسار هو 100,110,111. إذن، يكون قرار فك التشفير هو التحرك إلى المرحلة 110 ويكون فك تشفير الإحداثي الثاني من الرسالة هو الإحداثي 1.

تمرين

(**٨,٣,١**) لتكن C شفرة تلاف من النوع (2,1,3) حيث مولّداها هما $g_1(x) = 1 + x + x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$ (تم إنشاء مخطط مراحل C في التمرين (**٨ ، ٢ ، ١٢**)). فُك تشفير أول 4 إحداثيات من إحداثيات الكلمة المستقبلة $w = 11\ \ 00\ \ 00\ \ 00\ \ \cdots \leftrightarrow 1 + x = w(x)$ وذلك باستخدام جداول مماثلة للجدولين المقدمين في الشكلين (**٨,٧**) و (**٨,٨**) عندما يكون زمن الانتظار قبل البدء بفك التشفير هو:

(أ) تكّتان (ب) ثلاث تكّات (ج) أربع تكّات.

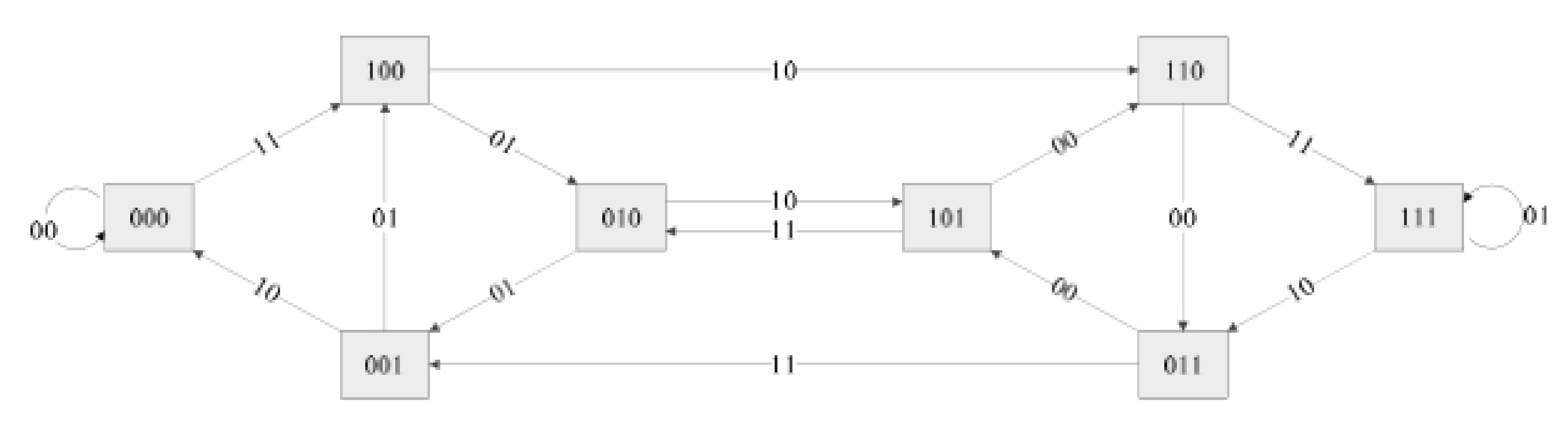
في حالة وجود مسارين هما الأقرب بحيث يكون التحرك إلى المرحلة التالية غير واضح فضع * في مكان فك تشفير إحداثي الرسالة ومن ثم افترض أن إحداثي الرسالة في هذه الحالة هو 0 لكي تتمكن من معرفة المرحلة التالية.

إذا قرّرنا الانتظار τ خطوة قبل بدء عملية فك التشفير فيكون قرار فك التشفير هو دراسة جميع المسارات ذات الطول τ التي تبدأ من المرحلة الحالية ومقارنة كل من هذه المسارات مع معلومات τ تكّة التي بحوزتنا من الكلمة المستقبلة. بعد ذلك نقوم بالتحرك

إلى المرحلة التالية في جميع المسارات الأكثر قُرباً إلى w. ومن ثم نستقبل تكّة أخرى من w قبل الانتقال إلى الخطوة التالية. أيضاً، وكما هو الحال عند التكّة الثانية عندما $\tau = 1$، إذا وجد مساران إلى w تكّة مستقبلة من الكلمة w يختلفان في القرار الذي يجب اتخاذه فنقوم باتخاذ قرار اعتباطي للتحرك إلى إحدى المراحل التالية. تُسمى خوارزمية فك التشفير هذه، **خوارزمية الاستنفاد لفك تشفير (Exhaustive Decoding Algorithm)** شفرات التلاف (لأنه قد تم دراسة جميع المسارات من الطول τ التي تبدأ من المرحلة الحالية قبل فك تشفير كل من إحداثيات الرسالة). كما يُسمى العدد τ، **سعة النافذة (Window Size)**؛ لأن τ هو كمية المعلومات التي لدينا من الكلمة w عند الشروع في اتخاذ قرار فك التشفير.

من الواضح أن مقدار زمن الانتظار قبل بدء عملية فك التشفير له تأثير على اختيارنا للكلمة الأقرب إلى كلمة الشفرة. والمسألة الآن تتلخص فيما إذا كان بالامكان إيجاد وسط مناسب بين اتخاذ قرار فك التشفير عند كل تكّة ساعة وبين فك التشفير بعد معرفة جميع إحداثيات الكلمة المستقبلة بحيث يكون باستطاعتنا تصويب بعض أنماط الأخطاء. ولكن ذلك يطرح السؤال التالي: ما هي الأخطاء الممكن تصويبها؟ سنحصل على عدد من الإجابات لهذا السؤال ونناقش الفترة الزمنية اللازمة قبل بدء فك التشفير لكل من هذه الاجابات.

نحتاج أولاً لدراسة مسألة أخرى. لنفرض أن C شفرة تلاف من النوع (2,1,3) لها المولّدان $g_1(x) = 1 + x^3$ و $g_2(x) = 1 + x + x^2$. الشكل (٨,٩) يُبيّن مخطط المراحل لهذه الشفرة.



الشكل (٨,٩). مخطط المراحل لشفرة تلاف إخفاقية.

لنفرض أن كلمة الشفرة المرسلة هي كلمة الشفرة الصفرية وأن الرسالة المقابلة لها هي $m = 000\cdots$ وأن الكلمة المستقبلة هي:

$$.w = 11\ \ 10\ \ 00\ \ 00\ \ \cdots \leftrightarrow 1 + x + x^2 = w(x)$$

فك تشفير w عملية سهلة؛ لأن w هي كلمة شفرة في هذه الحالة وهذا ما يؤكده مخطط المراحل باتباع المسار الذي يمر بالمراحل:

$$.000,100,110,011,101,110,\cdots$$

حيث افترضنا مسبقاً في هذه الحالة عدم وقوع أخطاء أثناء عملية الإرسال ومن ثم سنفترض أن الرسالة الأقرب هي $m = 110110\cdots \leftrightarrow \sum_{i=0}^{\infty}(x^{3i} + x^{3i+1})$ وهذا وضع خطير جداً؛ لأنه قد وقع خطأ في إرسال أول ثلاث إحداثيات افترضنا أن $c = 00\ \ 00\ \ \cdots$ هي الكلمة المرسلة) وهذا يقودنا إلى الوقوع في عدد غير منته من الأخطاء أثناء فك التشفير؛ (لأننا قمنا بفك تشفير $m = 110110\cdots$ عوضاً عن فك تشفير $m = 000000\cdots$). ومع ذلك فمن السهل أن نرى أن المشكلة هنا تكمن في وجود دورة في مخطط المراحل (مختلفة عن العروة التي عند المرحلة الصفرية) حيث إن مخرجات الأضلاع الموجّهة لهذه الدورة مُعلّمة بالأصفار. وهذا هو السبب؛ لأن وقوع عدد منته من الأخطاء أثناء عملية الإرسال ينتج عنه عدد غير منته من أخطاء فك التشفير. إذا عرفنا وزن مسار (أو دورة) في مخطط المراحل على أنه وزن مخرجات الأضلاع الموجّهة لهذا المسار، فإننا نعرّف **شفرة التلاف الإخفاقية** (**Catastrophic Convolutional Code**) على أنها شفرة التلاف التي يحتوي مخطط مراحلها على دورة وزنها صفر مختلفة عن العروة التي عند المرحلة الصفرية. من الممكن اثبات أن شفرة التلاف من النوع $(2,1,m)$ هي شفرة إخفاقية إذا كان $gcd(g_1(x), g_2(x)) \neq 1$. في شفرة التلاف هذه لدينا $g_1(x) = 1 + x^3 = (1 + x)(1 + x + x^2)$ ومن ثم نرى أن $.gcd(g_1(x), g_2(x)) = 1 + x + x^2 \neq 1$

تمرين

(**٨,٣,٢**) لكل من شفرات التلاف من النوع $(2,1,m)$ ، احسب $gcd(g_1(x), g_2(x))$ لتقرر فيما إذا كانت الشفرة اخفاقية. في حالة الشفرة الإخفاقية جد الدورة التي وزنها صفر (ومختلفة عن العروة التي عند المرحلة الصفرية) في مخطط مراحل الشفرة.

(أ) $g_1(x) = 1 + x$ و $g_2(x) = 1 + x + x^2 + x^3$.

(ب) $g_1(x) = 1 + x + x^4$ و $g_2(x) = 1 + x^2 + x^4$.

(ج) $g_1(x) = 1 + x + x^2$ و $g_2(x) = 1 + x + x^3 + x^4$.

فيما تبقى من هذا الفصل سنفرض أن الشفرات هي شفرات غير إخفاقية.

نرجع الآن إلى دراسة زمن الانتظار قبل البدء بعملية فك التشفير ومعرفة أنماط الأخطاء التي يمكن تصويبها. البداية الطبيعية لهذا الغرض هي إيجاد المسافة d لشفرة التلاف (تُسمى هنا المسافة الحرة الصغرى). لاحظنا سابقاً أن شفرة التلاف هي شفرة خطيّة وبهذا تكون مسافتها d هي أصغر أوزان كلمات الشفرة غير الصفرية. وبما أن دراستنا تقتصر على شفرات التلاف غير الإخفاقية فإن كلمة الشفرة غير الصفرية ذات الوزن المنتهي تقابل مساراً يخرج بداية من المرحلة الصفرية (لضمان وزن غير صفري لكلمة الشفرة) ومن ثم يعود بعد فترة معينة إلى المرحلة الصفرية ولا يخرج مرة أخرى (لضمان أن يكون وزن كلمة الشفرة منتهياً). لاحظ أن وزن أي مسار يخرج من المرحلة الصفرية في الشفرات غير الإخفاقية يجب أن يكون موجباً ؛ لعدم وجود دورات وزنها صفر عدا العروة التي عند المرحلة الصفرية. على سبيل المثال، وزن المسار $000,100,010,001,000,000,\cdots$ في الشكل (**٨,٦**) يساوي 6 ؛ لأنه يقابل كلمة الشفرة $11\ 10\ 01\ 11\ 00\ 00\ \cdots$ التي وزنها يساوي 6. كما أن المسار $000,100,110,111,011,001,000,000,\cdots$ يقابل كلمة الشفرة

$\cdots$ 00 00 11 10 00 00 01 11 ومن ثم فوزنه هو أيضاً يساوي 6. وبهذا تكون مسافة الشفرة C_1 هي $d(C_1) = 6$ (سنقدم في البند القادم خوارزمية لحساب $d(C)$).

تمرين

(**٨,٣,٣**) جد مسافة شفرات التلاف التي لها المولّدات التالية (مخططات المراحل لهذه الشفرات مقدمة في التمارين (**٨,٢,١١**)، (**٨,٢,١٢**)، (**٨,٢,١٣**)).

(أ) $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$.

(ب) $g_1(x) = 1 + x + x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$.

(ج) $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

بعد قيامنا بحساب مسافة الشفرة سنحاول تصويب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $\lfloor (d-1)/2 \rfloor$. ولكن علينا الاجابة الآن عن السؤال التالي: ما هو زمن الانتظار اللازم قبل البدء بفك التشفير؟ مسافة C_1 هي $d(C_1) = 6$ ومع ذلك عند استخدامنا خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau = 1$ وجدنا أن فك تشفير الكلمة المستقبلة $\cdots$ 00 11 $= w$ هي الكلمة $\cdots$ 00 00 00. ولهذا لم يتم تصويب نمط الخطأ w الذي وزنه يساوي 2 حيث $\lfloor (d(C_1) - 1)/2 \rfloor = 3 > 2$. ولكننا لو انتظرنا زمناً غير محدود لاستطعنا تصويب w إلى $\cdots$ 00 00.

يُعرف طول المسار على أنه عدد الأضلاع الموجهة في المسار (يُساهم الضلع الموجّه بعدد مرات وقوعه في المسار). إذا أردنا تصويب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن e فيجب أن يكون زمن الانتظار $\tau(e)$ اللازم من المرحلة الصفرية أكبر من $2e$. ولرؤية ذلك، نفرض أنه قد تم إرسال كلمة الشفرة الصفرية وأن عدد الأخطاء التي وقعت أثناء عملية الإرسال لا يزيد عن e (لاحظ أن شفرات التلاف هي شفرات خطيّة، ولذا يمكننا افتراض أن الكلمة الصفرية هي الكلمة التي تم

إرسالها دون المساس بالعمومية). باستخدام خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(e)$ نقوم بعد $\tau(e)$ تكّة ساعة بمقارنة العلامات لجميع المسارات من المرحلة الصفرية التي طولها $\tau(e)$ مع أول $\tau(e)$ تكّة من الكلمة المستقبلة w ومن ثم نختار أقرب المسارات لتحديد المرحلة التي يجب التحرك إليها. ولإجراء عملية فك تشفير صائبة يجب علينا اتخاذ قرار البقاء عند المرحلة الصفرية؛ لأننا قد فرضنا أن كلمة الشفرة المرسلة هي الكلمة الصفرية. ومن اختيار $\tau(e)$ نرى أن وزن جميع المسارات التي تغادر مباشرة المرحلة الصفرية لا يزيد عن $2e$ بعد عدد $\tau(e)$ من المراحل، وبهذا فهو يختلف عن أول $\tau(e)$ تكّة من w بأكثر من عدد e من المواقع.

من ناحية أخرى، وزن المسار الذي لا يغادر المرحلة الصفرية على الإطلاق يساوي صفراً ومن ثم فهو يبعد مسافة $wt(w) \leq e$ عن أول $\tau(e)$ تكّة من w.

إذن، لا يوجد أي مسار من المسارات التي تغادر مباشرة المرحلة الصفرية بحيث يكون هو الأقرب، ولذا فجميع المسارات الأقرب إلى w تتفق على البقاء عند المرحلة الصفرية بعد أول $\tau(e)$ تكّة. وكما لاحظنا عند دراستنا للشكلين (٨,٧) و (٨,٨) فإن عملية فك التشفير تتوقف إلى أن نستقبل تكّة أخرى من w. ولكن بعد استقبالنا لتكّة جديدة يكون بالإمكان تكرار النقاش السابق ونخلص إلى أن فك تشفير w صائب. في الحقيقة، من النقاش المقدّم سابقاً نكون قد برهنا أنه باستطاعتنا إجراء فك تشفير صائب للكلمة w إذا وقع عدد من الأخطاء لا يزيد عن e في أي $\tau(e)$ تكّة متتالية من الكلمة المستقبلة. بهذا نستطيع تصويب عدد غير منته من الأخطاء إذا كان عدد أخطاء $\tau(e)$ من التكّات المتتالية لا يزيد عن e (إن ذلك شبيه بوضع الشفرات القالبية ذات الطول المنتهي؛ لأنه يتم تصويب الأخطاء في مثل هذه الشفرات إذا كان عدد الأخطاء في أي من كلمات الشفرة لا يزيد عن e). وبهذا نكون قد عرفنا الزمن اللازم للانتظار.

لتكن C شفرة تلاف غير اخفاقية. لكل $1 \le e \le \lfloor (d-1)/2 \rfloor$ يُعرف $\tau(e)$ على أنه أصغر عدد صحيح x يحقق: جميع المسارات ذات الطول x في مخطط المراحل التي تغادر مباشرة المرحلة الصفرية لها وزن لا يزيد عن $2e$.

لاحظ أن تنفيذ خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(e)$ يحتاج إلى جميع المسارات من الطول $\tau(e)$ من المرحلة الحالية إلى كل من إحداثيات الرسالة المراد فك تشفيرها. ولكن إنشاء جميع هذه المسارات التي عددها $2^{\tau(e)}$ عند كل تكّة يستغرق فترة زمنية كبيرة، ولهذا سنقدم خوارزمية أسرع في البند (٨,٤). ولكن في الوقت الحالي لدينا المبرهنة التالية:

مبرهنة (٨,٣,٤)

لتكن C شفرة تلاف غير إخفاقية. لكل e حيث $1 \le e \le \lfloor (d-1)/2 \rfloor$، إذا وقع عدد من الأخطاء لا يزيد عن e في أي من أنماط الأخطاء ولكل $\tau(e)$ من الخطوات المتتالية أثناء عملية الإرسال فيكون باستطاعة خوارزمية الاستنفاد بنافذة سعتها $\tau(e)$ فك تشفير الكلمة المستقبلة بصورة صائبة. ■

مثال (٨,٣,٥)

لتكن C_1 شفرة التلاف التي لها المولّدان $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$ (الشكل (٨,٦) هو مخطط المراحل للشفرة C_1). بما أن $d(C_1) = 6$ فإننا ندرس الحالتين $e = 1$ و $e = 2$.

في الحالة $e = 1$ نرى أن جميع المسارات ذات الطول 2 التي تغادر مباشرة المرحلة الصفرية لها وزن أكبر من $2e = 2$. ويوجد على الأقل مسار واحد من الطول 1 يغادر مباشرة المرحلة الصفرية وزنه لا يزيد عن $2e$. إذن، $\tau(1) = 2$.

أما في الحالة $e = 2$ فنرى أن جميع المسارات ذات الطول 7 التي تغادر مباشرة المرحلة الصفرية لها وزن أكبر من $2e = 4$ (تحقق من ذلك!). ويوجد على الأقل مسار واحد طوله 6 يغادر مباشرة المرحلة الصفرية ووزنه لا يزيد عن $2e$. أحد هذه المسارات هو :

$$000,100,110,111,011,001,100$$

إذن، $\tau(2) = 7$ (الخوارزمية الأسرع التي سنقدمها في البند (٤,٨) تستطيع أيضاً حساب $\tau(e)$ بسرعة).

إذا استخدمنا خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(1)$ فإستناداً إلى المبرهنة (٤,٣,٨) نستطيع تصويب جميع أنماط الأخطاء التي تحتوي على عدد من الأخطاء لا يزيد عن $e = 1$ لأي $\tau(1) = 2$ تكّة متتالية. على سبيل المثال، نستطيع تصويب نمط الخطأ :

$$e_1 = 10\ \ 00\ \ 01\ \ 00\ \ 01\ \ 00\ \ 10\ \ \cdots.$$

وإذا استخدمنا خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(2)$ فمن الممكن تصويب جميع أنماط الأخطاء التي تحتوي على عدد من الأخطاء لا يزيد عن $e = 2$ لأي $\tau(2) = 7$ تكّة متتالية. على سبيل المثال، نستطيع تصويب نمط الخطأ :

$$e_2 = 11\ \ 00\ \ 00\ \ 00\ \ 00\ \ 00\ \ 00\ \ \cdots.$$

لاحظ أن المبرهنة (٤,٣,٨) لا تضمن لنا تصويب نمط الخطأ e_2 إذا اخترنا $e = 1$ (يوجد عدد $e < 2$ من الأخطاء عند التكّة الأولى لنمط الخطأ e_2).

كذلك، لا يمكن تصويب e_1 إذا اخترنا $e = 2$ (يوجد عدد $e < 4$ من الأخطاء عند أول $\tau(2) = 7$ تكّة متتالية لنمط الخطأ e_1). عند دراستنا للشفرات القالبية (ذات الطول المنتهي) لم نجد سبباً لكي يكون $e < \lfloor (d-1)/2 \rfloor$ ولكن يتحتم علينا عمل ذلك عند فك تشفير شفرات التلاف حيث نقوم باختيار e لنتمكن من تصويب نمط الخطأ المرجح وقوعه. ▲

تمارين

(**٨,٣,٦**) لكل من الشفرات C التالية ولكل e حيث $1 \le e \le \lfloor (d(C)-1)/2 \rfloor$ جد $\tau(e)$ (وجدنا $d(C)$ في التمرين (**٨,٣,٣**) ووجدنا مخططات المراحل في التمارين (**٨,٢,١١**)، (**٨,٢,١٢**)، (**٨,٢,١٣**)).

(أ) $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$.

(ب) $g_1(x) = 1 + x + x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$.

(ج) $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

(**٨,٣,٧**) ماذا يحدث لو حاولنا حساب $\tau(e)$ عندما يكون $e > \lfloor (d-1)/2 \rfloor$ ؟

(٨,٤) فك تشفير ڤيتربي المبتور
Truncated Viterbi Decoding

نقدم في هذا البند خوارزمية فك تشفير ڤيتربي المبتور لشفرات تلاف ثنائية من النوع $(2,1,m)$. نحتاج لتنفيذ هذه الخوارزمية إلى 2^m عملية حسابية وتخزين 2^m مساراً من الطول τ عند كل تكّة مقارنة مع 2^τ عملية حسابية وتخزين 2^τ مساراً من الطول τ عند تنفيذ خوارزمية الاستنفاد لفك التشفير. من الملائم هنا أنه عند التطبيق العملي للخوارزمية يتم اختيار سعة النافذة τ لتكون بين القيمتين $4m$ و $6m$ (هذا العدد غالباً ما يكون أكبر بكثير من $\tau(e)$). بُني هذا الاختيار على برهان احتمالي يُبيّن أن بهذا الاختيار لسعة النافذة يكون عدد أنماط الأخطاء التي لا يتم تصويبها قليل جداً. لهذا فإن تخزين 2^m مساراً عوضاً عن 2^τ مساراً يؤدي إلى توفير مناسب سواء في الزمن أو التخزين.

يعود السبب لتفضيل فك تشفير ڤيتربي المبتور على خوارزمية الاستنفاد لفك التشفير إلى أنه لكل مرحلة s يتم تخزين مسار واحد على الأكثر من الطول τ من المرحلة

الحالية إلى المرحلة s. نقوم أولاً بوصف مختصر لهذه الخوارزمية ثم نقدم بعد ذلك خطواتها بالتفصيل.

لنفرض أن $w = w_0, w_1, \cdots$ هي الكلمة المستقبلة. تذكّر أن w_i لكل $i \geq 0$ هي عديد من النوع n؛ لأننا استخدمنا التوريق البيني لتمثيل كلمات الشفرة والكلمات المستقبلة. وبما أننا نستخدم $n = 2$ فتتكون w_i من إحداثيين (يتم استقبال الإحداثيين عند الزمن i).

جميع المسارات من المرحلة الصفرية لا تزال مخزّنة عند أول m تكّة. ولكن عند الزمن m يوجد 2^m مساراً كل منها ينتهي عند مرحلة مختلفة، ولهذا فإن $t = m$ هي المرة الأولى التي ينتهي بها مسار واحد فقط عند كل مرحلة. وأثناء إنشاء 2^m من المسارات تقوم الخوارزمية بحساب المسافة بين مخرج المسار والكلمة المستقبلة وتخزن هذه المسافة مع المسار. عند $t > m$ يوجد لكل مرحلة $s = s_0, s_1, \cdots, s_{m-1}$ مرحلتان ينطلق من كل منهما ضلع موجّه إلى s وهاتان المرحلتان هما:

$S_0 = s_1, s_2, \cdots, s_{m-1}, 0$ و $S_1 = s_1, s_2, \cdots, s_{m-1}, 1$.

عند $t = m$ تقوم الخوارزمية بتخزين المسارين W_0 و W_1 من المرحلة الحالية إلى المرحلتين S_0 و S_1 على التوالي مع المسافتين $d(S_0, t)$ و $d(S_1, t)$ من المسارين W_0 و W_1 على التوالي إلى الكلمة المستقبلة. عند $t > m$ وعند التكّة t تقوم الخوارزمية بجمع المسافتين بين w_{t-1} ومخرجات الضلعين الموجهين من S_0 وS_1 إلى s مع المسافتين $d(S_0, t-1)$ و $d(S_1, t-1)$ على التوالي وتأخذ المجموع الأصغر ليكون المسافة $d(s, t)$ بين امتداد المسار W_0 أو W_1 (أيهما يُعطي مسافة أصغر) والمرحلة s.

يتم تخزين المسارات كمتتالية من الإحداثيات المستقبلة وليس على صورة متتالية من المراحل أو متتالية من مخرجات الأضلاع الموجّهة. في اللحظة التي يكون فيها $t \geq \tau$ يتم فك تشفير إحداثي رسالة عند كل تكّة. ويتم التعامل مع المراحل ذات المسافات

$d(s,t)$ الصغرى: إذا اتفقت المسارات المخزّنة في كل مرحلة من هذه المراحل على المرحلة التالية للحركة (أي أن تحتوي المسارات على نفس إحداثي الرسالة السابقة) فعند ذلك يتم فك تشفير إحداثي الرسالة هذه. وإذا لم تتفق جميع المسارات فنقوم بتعليم إحداثي الرسالة المراد فك تشفيرها بالعلامة * (من الممكن فك تشفير هذا الإحداثي إلى 0 ولكن من المناسب توضيح أن أياً من الإحداثيين ليس هو المفضل). بعد اتخاذ قرار بشأن إحداثي الرسالة يتم حذفها من جميع المسارات المخزنة. ومن ثم ينقص طول المسارات المخزنة إلى $\tau - 1$ ولكن يتم زيادة هذا الطول ليصبح τ عند تمديد هذه المسارات عند التكّة $\tau + 1$.

خوارزمية (٨,٤,١) [خوارزمية ڤيتربي المبتورة لفك تشفير شفرات تلاف من النوع $(n,1,m)$ بنافذة سعتها τ]

لتكن $w_0w_1\cdots$ هي الكلمة المستقبلة. يتم تنفيذ الخطوات التالية:

(١) (خطوة البداية) إذا كان $t = 0$ فنعرّف $W(s;t)$ و $d(s;t)$ على النحو التالي:

$$W(s;t) = s**\cdots* \quad \text{(طولها } \tau\text{)}$$

$$d(s;t) = \begin{cases} 0 \;, & \text{إذا كانت } s \text{ هي المرحلة الصفرية} \\ \infty \;, & \text{خلاف ذلك} \end{cases}$$

(٢) (حساب المسافة) لكل $t > 0$ ولكل مرحلة $s = s_0, s_1, \cdots, s_{m-1}$ نعرف:

$$d(s;t) = min\{d(s_1,s_2,\cdots,s_{m-1},0;t-1) + d(s_1,s_2,\cdots,s_{m-1},1;t-1) + d_1(s)\}$$

حيث $d_i(s)$ هي المسافة بين w_{t-1} ومخرج الضلع الموجّه من $s_1,s_2,\cdots,s_{m-1},i$ إلى s.

(٣) (حساب المسارات)

(أ) إذا كان:

$$d(s_1,\cdots,s_{m-1},i;t-1) + d_i(s) < d(s_1,\cdots,s_{m-1},j;t-1) + d_j(s)$$

حيث $\{i,j\} = \{0,1\}$ فنكوّن $W(s;t)$ من $W(s_1,\cdots,s_{m-1},0;t-1)$ وذلك باضافة الإحداثي الواقع أقصى يسار s إلى يسار $W(s_1,\cdots,s_{m-1},0;t-1)$ ثم نحذف الإحداثي الواقع في أقصى اليمين.

(ب) إذا كان:

$$d(s_1,\cdots,s_{m-1},0;t-1)+d_0(s)=d(s_1,\cdots,s_m;t-1)+d_1(s)$$

فنكوّن $W(s;t)$ من $W(s_1,\cdots,s_{m-1},0;t-1)$ وذلك بإضافة الإحداثي الواقع أقصى يسار s إلى يسار $W(s_1,\cdots,s_{m-1},0;t-1)$.

(٤) (فك التشفير) لكل $t \geq \tau$، ضع {لكل مرحلة $S(t)=\{s: d(s;t) \leq$ s' ، $d(s';t)$. إذا كان إحداثي أقصى اليمين في المسار $W(s;t)$ وليكن i هو نفسه لجميع $s\epsilon S(t)$ فنقوم بفك تشفير إحداثي الرسالة على أنه i وخلاف ذلك يكون فك إحداثي الرسالة على أنه *.

ملحوظة

لاحظ أن الإحداثيات التي عددها m في أقصى يسار $W(s;t)$ يجب أن تساوي s ومن ثم لا توجد حاجة إلى تخزينها.

يقدم التمرين (**٨,٤,٦**) تعميماً للخوارزمية (**٨,٤,١**) لفك تشفير شفرات تلاف من النوع (n,k,m).

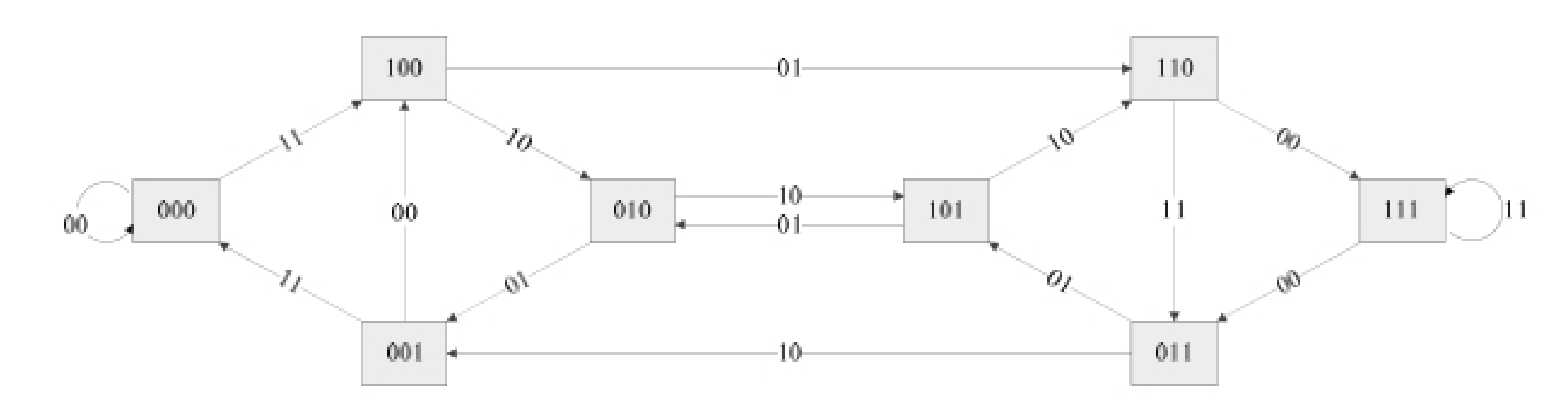
مثال (٨,٤,٢)

لتكن C_1 الشفرة التي لها المولّدان $g_1(x)=1+x+x^3$ و $g_2(x)=1+x^2+x^3$.

ولتكن:

$$w=w_0w_1w_2\cdots=11\ 00\ 00\ \cdots \leftrightarrow 1+x$$

هي الكلمة المستقبلة (سبق وأن درسنا هذا المثال بشيء من التفصيل في البند (**٨,٣**)). ولنفرض أن سعة النافذة هي $\tau=\tau(2)=7$ (انظر المثال (**٨,٣,٥**)). مخطط المراحل للشفرة C_1 هو المبين في الشكل (**٨,١٠**).



الشكل (٨,١٠). مخطط مراحل الشفرة C_1.

عنـد $t = 0$: نضـع $W(s;0) = s****$ لكـل مرحلـة s ونعـرف $d(000;0)$ و $d(s';0) = \infty$ لكل مرحلة s' مختلفة عن المرحلة الصفرية.

عند $t = 1$: $w_{t-1} = w_0 = 11$. استناداً إلى الخطوة (٢) من الخوارزمية (**٨,٤,١**) نقوم بدراسة جميع المراحل، مرحلة مرحلة.

: $s = 000$

$$d(000;1) = min\{d(000;0) + 2, d(001;0) + 0\}$$
$$= min\{2, \infty\}$$
$$= 2$$

(نحصل على $d_0(000) = 2$ بملاحظة أن مخرج الضلع الموجّه من المرحلة 000 إلى المرحلة 000 هو 00 وهذا يختلف عن $w_0 = 11$ بموقعين. وبالمثل، $d_1(000) = 0$ ؛ لأن مخرج الضلع الموجّه من المرحلة 001 إلى المرحلة 000 هو 11 وهذا لا يختلف عن w_0).

باستخدام الترميز المستخدم في الخطوة (٣أ) من الخوارزمية (**٨,٤,١**) نجد أننا نحصل على القيمة الصغرى عند $i = 0$، وبهذا نحصل على $W(000;1)$ من $W(000;0)$ بإضافة الإحداثي الذي يقع أقصى يسار المرحلة 000 إلى $W(000;0) = 000****$ وبعد ذلك نقوم بحذف الإحداثي الواقع في أقصى اليمين. إذن، $W(000;1) = 0000***$.

: $s = 100$

$$d(100;1) = min\{d(000;0) + d_0(100), d(001;0) + d_1(100)\}$$
$$= min\{0 + 0, \infty + 2\} = 0$$

وفي هذه الحالة أيضاً نحصل على القيمة الصغرى عند $i = 0$ ، وبهذا نحصل على $W(100;1)$ من $W(000;0)$ باضافة الإحداثي الواقع في أقصى يسار المرحلة $s = 100$ إلى $W(000;0)$ ومن حذف الإحداثي الواقع في أقصى اليمين فيكون $W(100;1) = 1000***$.

$s = 010$:

$$\begin{aligned} d(010;1) &= min\{d(100;0) + d_0(010), d(101;0) + d_1(010)\} \\ &= min\{\infty + 1, \infty + 1\} \\ &= \infty \end{aligned}$$

في هذه الحالة نستخدم الخطوة (٣ب) ؛ لأننا نحصل على قيمة صغرى في كلا الحدّين. لدينا :

$$W(100;0) = 100****$$
$$W(101;0) = 101****$$

ومن ثم فإن $W(010;1) = 010****$.

الإحداثي الرابع في المسار $W(010;1)$ هو * لأن $W(100;0)$ و $W(101;0)$ يختلفان في هذا الموقع.

بالمثل ، من الممكن حساب $W(s;t)$ و $d(s;t)$ لبقية المراحل. الجدول التالي يلخص لنا الحسابات التي أجريناها :

المرحلة s	$t = 0$	$t = 1$
000	$0{,}000****$	$2{,}0000***$
100	$\infty, 100****$	$0{,}1000***$
010	$\infty, 010****$	$\infty, 010****$
110	$\infty, 110****$	$\infty, 110****$
001	$\infty, 001****$	$\infty, 001****$
101	$\infty, 101****$	$\infty, 101****$
011	$\infty, 011****$	$\infty, 011****$
111	$\infty, 111****$	$\infty, 111****$

(كل مدخل في الجدول السابق هو $(d(s;t), W(s;t)$).

لاحظ أن تمثيل مخطط المراحل في الجدول السابق يُبيّن إلى جانب المرحلة s مخرج الأضلاع الموجّهة إلى s في مخطط المراحل. وهذه هي بالضبط المخرجات التي نحتاج إليها لحساب $d_0(s)$ و $d_1(s)$، وبهذا نرى أهمية هذه الجدولة للمعلومات وسنظهرها في الجداول التي تلي.

باستمرار فك التشفير عند $t = 2$ و $t = 3$ نحصل على الجدول التالي (لاحظ هنا أن $w_1 = 00$ و $w_2 = 00$).

المرحلة	المخرج			
$s = X_0X_1X_2$	$X_3 = 0$	$X_3 = 1$	$t = 2$	$t = 3$
000	00	11	2,00000 **	2,000000 *
100	11	00	4,10000 **	4,100000 *
010	10	01	1,01000 **	5,010000 *
110	01	10	1,11000 **	5,110000 *
001	01	10	∞, 001 ****	2,001000 *
101	10	01	∞, 101 ****	2,101000 *
011	11	00	∞, 011 ****	3,011000 *
111	00	11	∞, 111 ****	1,111000 *

لاحظ أننا وصلنا الآن إلى $t = 3 = m$. وفي هذه الحالة لدينا $d(s;t) < \infty$ لجميع المراحل s. وهذا يعني وجود مسار طوله m من المرحلة الصفرية إلى كل من المراحل الأخرى. لحد الآن، وجدنا عند حسابنا للقيمة الصغرى باستخدام الخطوة (٢) من الخوارزمية (**٨,٤,١**) أن إحدى القيمتين هي ∞. وهذا ليس صحيحاً عندما يكون $t > m$.

عند $t = 4$: $w_3 = 00$ وبدراسة المراحل نجد أن:

: $s = 000$

$$\begin{aligned} d(000;4) &= min\{d(000;3) + d_0, d(001;3) + d_1\} \\ &= min\{2 + 0{,}2 + 2\} \\ &= 2 \end{aligned}$$

ونحصل على القيمة الصغرى عند $i = 0$ ومن ثم نحصل على $W(000;4)$ من $W(000;3)$. إذن:

$$.W(000;4) = 0000000$$

$:s = 100$

$$\begin{aligned} d(100;4) &= min\{d(000;3) + d_0, d(001;3) + d_1\} \\ &= min\{2 + 2,2 + 0\} \\ &= 2 \end{aligned}$$

حيث نحصل على القيمة الصغرى عند $i = 1$ ومن ثم نحصل على $W(100;4)$ من $W(001;3)$ ويكون $W(100;4) = 1001000$.

$:s = 010$

$$\begin{aligned} d(010;4) &= min\{d(100;3) + d_0, d(101;3) + d_1\} \\ &= min\{4 + 1,2 + 1\} \\ &= 3 \end{aligned}$$

(حيث المسافة d_0 هي المسافة بين w_3 ومخرج الضلع الموجّه من المرحلة 100 إلى المرحلة 010 ومن ثم فإن $d_0 = 1$. أيضاً، d_1 هي المسافة بين w_3 ومخرج الضلع الموجّه من المرحلة 101 إلى المرحلة 100 ومن ثم فإن $d_1 = 1$.). إذن، نحصل على $W(010;4)$ من $W(101;3)$ ويكون $W(010;4) = 0101000$.

وبحساب مماثل لكل من المراحل الأخرى نحصل على:

المرحلة	المخرج		
s	$X_3 = 0$	$X_3 = 1$	$t = 4$
000	00	11	2,0000000
100	11	00	2,1001000
010	10	01	3,0101000
110	01	10	3,1101000
001	01	10	4,0011000
101	10	01	4,1011000
011	11	00	1,0111000
111	00	11	3,1111000

عند $t = 5$: $w_4 = 00$ وندرس كل مرحلة من المراحل.

$s = 000$:

$$
\begin{aligned}
d(000;5) &= min\{d(000;4) + d_0, d(001;4) + d_1\} \\
&= min\{2 + 0{,}4 + 2\} \\
&= 2
\end{aligned}
$$

ويكون $W(000;5) = 0000000$.

$s = 100$:

$$
\begin{aligned}
d(100;5) &= min\{d(000;4) + d_0, d(001;4) + d_1\} \\
&= min\{2 + 2{,}4 + 0\} \\
&= 4
\end{aligned}
$$

في هذه الحالة، لدينا $d(000;4) + d_0 = d(001;4) + d_1$. ومن ذلك نرى استناداً إلى الخطوة (٣ب) أننا نحصل على $W(100;5)$ من كل من $W(000;4)$ و $W(001;4)$ بوضع * عندما يختلفان وإضافة الإحداثي أقصى يسار 100 وحذف الإحداثي الواقع في أقصى اليمين. وبما أن $W(000;4) = 0000000$ وأن $W(001;4) = 0011000$ فيكون:

$W(100;5) = 100 ** 00$.

وبالاستمرار على هذه الشاكلة لبقية المراحل ومن الحالتين $t = 6$ و $t = 7$ نحصل على الجدول التالي:

المرحلة	المخرج				
s	$X_3 = 0$	$X_3 = 1$	$t = 5$	$t = 6$	$t = 7$
000	00	11	2,0000000	2,0000000	2,0000000
100	11	00	4,100 ** 00	2,1001110	4,100 ****
010	10	01	3,0100100	3,0101110	3,0100111
110	01	10	3,1100100	3,1101110	3,1100111
001	01	10	2,0011100	4,001 ** 10	4,001 * 1 * 1
101	10	01	2,1011100	4,101 ** 10	4,101 * 1 * 1
011	11	00	3,0111100	3,0111010	3,0111001
111	00	11	3,1110100	3,1110010	3,1110111

أخيراً وصلنا إلى الحالة $t = \tau$. نستطيع الآن فك تشفير إحداثي الرسالة الأول باستخدام الخطوة (٤) من الخوارزمية (٨,٤,١). في هذه الحالة لدينا $S(7) = \{000\}$؛ لأن $d(000; 7) = 2 < d(s; 7)$ لجميع المراحل $s \neq 000$. وبهذا يكون أول إحداثي يفك تشفيره هو الإحداثي الواقع في أقصى اليمين للمسار $W(000; 7)$، أي الإحداثي 0. الآن، نقوم بحذف الإحداثي الواقعة في أقصى اليمين للمسار $W(s; 7)$ عند $t = 8$ وذلك أثناء انشاء $W(s; 8)$ (الخطوة (٣) من الخوارزمية (٨,٤,١)).

الجدول التالي يُبيّن فك التشفير لبعض التكّات الأخرى:

المرحلة s	$t = 8$	$t = 9$	$t = 10$	$t = 11$	$t = 12$
000	2,0000000	2,0000000	2,0000000	2,0000000	2,0000000
100	4,100 ****	4,100 ** * 0	4,100 ****	4,100 ** * 0	4,1000000
010	5,010 ****	5,010 ****	5,010 ****	5,010 ****	5,0100 ***
110	5,110 ****	5,110 ****	5,110 ****	5,110 ****	5,1100 ***
001	4,001 ****	4,0011101	4,0011100	6,001 ****	6,001 ****
101	4,101 ****	4,1011101	4,1011100	6,101 ****	6,101 ****
011	3,0111011	3,0111001	5,0111 ***	5,01110 **	5,01110 **
111	3,1110011	5,111 ****	5,1110 ***	5,1110 ***	5,1110 ***
فك التشفير إلى:	0	0	0	0	0

▲

مثال (٨,٤,٣)

مرة أخرى نأخذ الشفرة C_1 المقدمة في المثال (٨,٤,٢). لنفرض أن:

$$w = 11\ 00\ 00\ 00\ 10\ 00\ \cdots \leftrightarrow 1 + x + x^8$$

هي الكلمة المستقبلة. ومرة أخرى نستخدم الخوارزمية (٨,٤,١) بنافذة سعتها $\tau(2) = 7$ (انظر المثال (٨,٣,٥)). الحسابات هي تكرار للحسابات التي أجريناها في المثال (٨,٤,٢) إلى أن تصل الحالة $t = 5$ حيث يبدأ تأثير الحد x^8 في الكلمة $w(x)$.

المرحلة	المخرج					
s	$X_3 = 0$	$X_3 = 1$	$t = 4$	$t = 5$	$t = 6$	$t = 7$
000	00	11	2,0000000	3,0000000	3,000 *** 0	3,0000 ***
100	11	00	2,1001000	3,1000000	1,1001110	3,1001001
010	10	01	3,0101000	2,0100100	4,010 *** 0	2,0100111
110	01	10	3,1101000	4,110 * 100	4,110 *** 0	2,1100111
001	01	10	4,0011000	1,0011100	3,0010010	5,001 ****
101	10	01	4,1011000	3,101 * 100	3,1010010	5,101 ****
011	11	00	1,0111000	4,011 * 100	4,0111 * 10	4,01110 * 1
111	00	11	3,1111000	4,111 * 100	4,1110 * 10	4,1110 ***
فك التشفير إلى :						1

في هذه الحالة، عند $t = 7$ نقوم بفك تشفير الإحداثي 1 من الرسالة. إذا فرضنا أن الكلمة الصفرية هي الكلمة التي تم إرسالها فيكون الخطأ الثالث في الكلمة $w(x)$ هو الذي تسبب في فك تشفير خاطئ. ▲

تمارين

(**٨,٤,٤**) استمر في فك تشفير $w(x)$ المقدمة في المثال (**٨,٤,٣**) عند $t = 8,9,10,11,12$.

هل من الممكن أن يكون إحداثي الرسالة التي تم فك تشفيرها هو 0 عندما يكون $t \geq 12$ ؟

(**٨,٤,٥**) مرة أخرى، استخدم شفرة التلاف C_1 حيث $g_1 = 1 + x + x^3$ و $g_2 = 1 + x^2 + x^3$ واستخدم الخوارزمية (**٨,٤,١**) بنافذة سعتها $\tau(2) = 7$ لفك تشفير كل من الكلمات المستقبلة التالية. استمر في عملية فك التشفير حتى $t = 9$.

(أ) $w(x) = 1 + x^3 \leftrightarrow 10\ 01\ 00\ 00\ \cdots$.

(ب) $w(x) = 1 + x + x^2 \leftrightarrow 11\ 10\ 00\ 00\ \cdots$.

(ج) $w(x) = x^3 + x^8 + x^{12} \leftrightarrow 00\ 01\ 00\ 00\ 10\ 00\ 10\,00\ \cdots$.

(٨,٤,٦) يمكن تعميم الخوارزمية (٨,٤,١) لفك تشفير شفرات تلاف من النوع (n, k, m) على النحو التالي (مخططات المراحل لهذه الشفرات هي المقدمة في التمرين (٨,٢,١٤)).

(١) نفس خطوة الخوارزمية (٨,٤,١).

(٢) لكل $t > 0$ ولكل مرحلة $s_0, s_1, \cdots, s_{m-k}$ نعرف :

$$d(s;t) = \min_u \{d(s_k, \cdots, s_{m-k}, u; t-1) + d_u\}$$

حيث مجال u هو جميع الكلمات الثنائية من الطول k وحيث d_u هي المسافة بين w_{t-1} ومخرج الضلع الموجّه من المرحلة $s_k, \cdots, s_{m-k}, u$ إلى المرحلة s في مخطط المراحل.

(٣) (أ) إذا كان لكل $v \neq u$

$$d(s_k, \cdots, s_{m-k}, u; t-1) + d_u < d(s_k, \cdots, s_{m-k}, v; t-1) + d_v$$

فنقوم بإنشاء $W(s;t)$ من $W(s_k, \cdots, s_{m-k}, u; t-1)$ بحذف الإحداثيات التي عددها k في أقصى اليمين وإضافة الإحداثيات التي عددها k في أقصى يسار s إليه.

(ب) إذا لم تكن $d(s_k, \cdots, s_{m-k}, u; t-1)$ هي القيمة الصغرى لخيار وحيد u فنقوم بإنشاء $W(s;t)$ باختيار أي من القيم u ومن ثم نستمر كما في الخطوة (٣أ). من الممكن أيضاً أن نأخذ تركيباً لجميع المسارات $W(s_k, \cdots, s_{m-k}, u; t-1)$ التي تكون فيها المسافة $d(s_k, \cdots, s_{m-k}, u; t-1)$ مسافة صغرى (كما هو الحال في الخوارزمية (٨,٤,١))، ومن ثم نضع العلامة * في المواقع التي يختلف فيها مساران.

(٤) لكل $t \geq \tau$، ضع $S(t) = \{s: d(s;t) \leq d(s';t)$ لجميع المراحل $s'\}$.

فك تشفير إحداثيات الرسالة $m_{1,t}, m_{2,t}, \cdots, m_{k,t}$ حيث $m_{i,t}$ هو الإحداثي i من الإحداثيات k الواقعة في أقصى يمين $W(s;t)$ لكل $s \epsilon S(t)$. وإذا اختلف مساران في الموقع i يكون فك التشفير هو $m_{i,t} = *$.

برهن أن هذه الخوارزمية هي بالفعل تعميم للخوارزمية (**٨,٤,١**).

نناقش بعض الملاحظات على الخوارزمية (**٨,٤,١**). أولى هذه الملاحظات هي إمكانية وجود طرق أخرى لتعريف خطوة فك التشفير (الخطوة (٤) من الخوارزمية). على سبيل المثال، من الممكن عدم البدء بعملية فك التشفير حتى تتفق جميع المسارات إلى كل من المراحل في الإحداثي الواقع في أقصى اليمين (أي الإحداثي المستخدمة في فك التشفير). ولكن في مثل هذه الحالة يجب علينا انتظار عدد كبير من التكّات قبل تنفيذ فك التشفير وهذا يحتاج إلى سعة تخزين أكبر. من الممكن أيضاً إجراء تعديل آخر على الخطوة (٤) وهو حذف كل من المسارات التي تختلف فيها الإحداثي الواقع في أقصى اليمين عن إحداثي الرسالة الجاري فك تشفيره؛ (لأن مثل هذه المسارات تتحرك إلى مراحل مختلفة). ولكن مثل هذه الإجراء سيطرح بعض الأسئلة النظرية عن الخوارزمية حيث من الممكن أن يؤدي فك التشفير في هذه الحالة إلى عدد غير منته من الأخطاء في أنماط أخطاء اندفاعية منتهية أثناء عملية الإرسال.

أما ثاني هذه الملاحظات فهي السؤال: هل من الممكن إثبات نتيجة مماثلة للمبرهنة (**٨,٣,٤**) لخوارزمية ڤيتربي المبتورة لفك التشفير (خوارزمية (**٨,٤,١**))؟ الاجابة عن هذا السؤال هي لا؛ لأن هذه الخوارزمية تحتاج إلى بعض الوقت لكي تتخلص من الأخطاء التي يمكن وقوعها في كلمة الشفرة أثناء عملية الإرسال. ولرؤية لماذا يوجد فرق بين الخوارزميتين، افرض أن $t = 2$ في المثال (**٨,٤,٢**). عند استخدام خوارزمية ڤيتربي المبتورة لفك التشفير فإن المسار الذي ينتظر في المرحلة 000 سيتذكر الخطأين اللذين سبق وقوعهما في w عند التكّة $t = 1$ عندما كانت $w_{t-1} = 11$ والسبب في ذلك يعود إلى أن $d(000;2) = 2$. سنرى في المثال (**٨,٤,٧**) أن تأثير هذين الخطأين سيبقى حتى التكّة $t = 12$. ولكن من ناحية أخرى، عند استخدام خوارزمية الاستنفاد لفك التشفير نرى أن الخطأين اللذين كان لهما تأثير في قرار فك التشفير عند التكّة

$t = 1$ ينتهي تأثيرهما بعد ذلك (أي عند $t \geq 2$). تذكر أنه عند $t \geq 2$ يتم مقارنة المسارات ذات الطول τ من المرحلة 000 مع $w_{t-1}, w_t, \cdots, w_{t+\tau-2} = 00 \cdots 0$ وهذا جزء من الكلمة المستقبلة يتفق فقط مع المسارات التي لا تزال عند المرحلة الصفرية.

نقدم الآن بعض التفصيلات عن الزمن الذي يستمر فيه تأثير الأخطاء أثناء عملية الإرسال على فك التشفير عند استخدام خوارزمية ڤيتربي المبتورة لفك التشفير بنافذة سعتها $\tau(e)$ المعرفة في الخوارزمية (**٨,٤,١**). نبدأ بتقديم بعض التعريفات. نفرض أن $w(s, s')$ هو الوزن الأصغر لمر من s إلى s' في مخطط المراحل. لنفرض أن $s(t)$ هي المرحلة الصحيحة عند التكّة t (أي أن $s(t)$ هي مرحلة وصول كلمة الشفرة المرسلة عند التكّة t). سنقول إن فك التشفير جاهز من **النوع** $\boldsymbol{e}$ (**e-ready**) عند التكّة t إذا تحقق الشرطان التاليان:

(١) $d(s'; t) \geq d(s(t); t) + min\{1 + e, w(s(t), s')\}$ لكل $s' \neq s(t)$.

(٢) إذا كان $w(s(t), s') < 1 + e$ فإن $W(s'; t) = s'v$ (من الطول τ)حيث v يحقق $W(s(t); t) = s(t)v$.

مثال (٨,٤,٧)

في المثال (**٨,٤,٢**)، نرى أن المرحلة الصحيحة لكل $t \geq 1$ هي $s(t) = 000$؛ لأننا افترضنا أن كلمة الشفرة التي تم إرسالها هي الكلمة الصفرية. وبما أن $m = 3$ عدد صغير فيمكن حساب $w(s(t), s') = w(000, s')$ لكل $s' \neq 000$ من مخطط المراحل بسهولة:

$$w(000,100) = 2, w(000,010) = 3, w(000,001) = 4,$$
$$w(000,110) = 3, w(000,101) = 4, w(000,011) = 3,$$
$$w(000,111) = 3$$

المرة الأولى التي يكون عندها فك التشفير جاهزاً من النوع 2 في المثال (**٨,٤,٢**) هي عند التكّة $t = 12$. ولرؤية ذلك لاحظ ما يلي:

عند $t = 10$ ، لدينا :

$$d(001;10) = 4 < 5 = d(000;10) + min\{1 + e, w(000,001)\}$$

ولذا فالشرط (١) من تعريف جاهزية فك التشفير غير محقق.

عند $t = 11$ نرى أن جميع المراحل تحقق الشرط (١) من تعريف جاهزية فك التشفير ولكن $w(000,100) = 2 < 3 = 1 + e$ وأن $W(100;11) = 100 **** \neq 100v$ (لأن $W(000;11) = 0000000 = s(1)v$ وبهذا يكون $v = 0000$).

عند $t = 12$ نرى أن جميع المراحل تحقق الشرط (١) وأن $s' = 100$ هي المرحلة الوحيدة حيث $w(000, s') < 1 + e$ و $W(100;12) = 1000000 = s'0000 = s'v$. ▲

المبرهنة التالية تُبيّن أهمية أن يكون فك التشفير جاهزاً من النوع e.

مبرهنة (٨,٤,٨)

لتكن C شفرة تلاف غير إخفاقية تستخدم خوارزمية ڤيتربي المبتورة لفك التشفير (خوارزمية (**٨,٤,١**)). عند التكّة t ، إذا كان فك التشفير جاهزاً من النوع e فسنحصل على فك تشفير صائب إذا وقعت أخطاء لا يزيد عددها عن e أثناء عملية الإرسال.

توضح لنا المبرهنة خلفية تسمية الجاهزية من النوع e. ومن الواضح أن هذه المبرهنة أضعف بكثير من المبرهنة (**٨,٣,٤**). يُعرف **فضاء الحماية (Guard Space)** على أنه الفترة الزمنية الخالية من أخطاء الإرسال التي تلي أخطاء اندفاعية. للحصول على نتيجة مشابهة للمبرهنة (**٨,٣,٤**) نحتاج لمعرفة فضاء الحماية اللازم قبل أن يكون فك التشفير جاهزاً من النوع e. عند استخدام فك التشفير الاستنفادي، نرى أن المبرهنة (**٨,٣,٤**) تضمن لنا فضاء حماية يساوي 0 (إذا اعتبرنا أن الجاهزية من النوع e تعني أن أي نمط خطأ لاحق وزنه لا يزيد عن e يؤدي إلى فك تشفير صائب للكلمة المستقبلة). في الحقيقة، يمكن إثبات أن فضاء الحماية اللازم ليكون فك تشفير ڤيتربي المبتور جاهزاً من النوع e بعد أخطاء اندفاعية هو زمن منته وأنه من الممكن معرفة طول

فضاء الحماية لبعض شفرات التلاف التي يكون فيها العدد m صغيراً. إن أقرب صيغة للمبرهنة (٨,٣,٤) يمكن الحصول عليها هي:

مبرهنة (٨,٤,٩)

لتكن C شفرة تلاف غير اخفاقية تستخدم خوارزمية ڤيتربي المبتورة لفك التشفير بنافذة سعتها $\tau(e)$ (الخوارزمية (٨,٤,١)). إذا أمكن تجزئة أنماط الأخطاء إلى أخطاء اندفاعية وزن كل منها لا يزيد عن e حيث يتبع كل منها فضاء حماية طوله كافٍ (منته) فإن فك التشفير يكون صائباً.

تمارين

(**٨,٤,١٠**) (أ) استخدم الخوارزمية (**٨,٤,١**) بنافذة سعتها $\tau(2) = 6$ لفك تشفير الكلمة المستقبلة $w = 11\ 00\ 00\ \cdots \leftrightarrow 1 + x = w(x)$ المشفرة باستخدام شفرة تلاف من النوع (2,1,2) بمولّدين $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$. استمر في عملية فك التشفير لإثبات أن فك التشفير جاهز من النوع 2 عند $t = 10$ بفرض أن كلمة الشفرة التي تم إرسالها هي الكلمة الصفرية (ومن ثم فالمرحلة الصحيحة $s(t)$ هي المرحلة الصفرية لكل t).

(ب) أثبت أن فك التشفير ليس جاهزاً من النوع 2 عند $t = 9$ ومن ثم لا تضمن لنا المبرهنة (**٨,٤,٨**) تصويب أي نمط خطأ لاحق وزنه لا يزيد عن $e = 2$. إذا كان $t = 10$ و $t = 11$ فأثبت أن إحداثيات الكلمة المستقبلة يتغير كل منها إلى 10 (أي أن الكلمة المستقبلة هي $w(x) = 1 + x + x^{18} + x^{20}$) ومن ثم يكون فك التشفير * عند $t = 12$.

(**٨,٤,١١**) لكل كلمة مستقبلة في التمرين (**٨,٤,٥**)، جد أصغر t بحيث يكون فك التشفير جاهزاً من النوع 2 عند التكّة t.

أخيراً نقوم بحساب كل من $d(C)$ و $\tau(e)$. ولانجاز ذلك علينا إيجاد أوزان المسارات التي غادرت للتو المرحلة الصفرية. لحساب $d(C)$ نحتاج إلى إيجاد المسار ذي الوزن الأصغر ولحساب $\tau(e)$ نحتاج إلى إيجاد الطول x بحيث يكون وزن أي مسار طوله على الأقل x لا يزيد عن $2e$. من الممكن تعديل خوارزمية ڤيتربي المبتورة لفك التشفير (الخوارزمية (٨,٤,١)) لانجاز المهمتين. لنفرض أولاً أن الكلمة الصفرية هي الكلمة المرسلة. عندئذ، دالة المسافة تحسب لنا أوزان المسارات. ثانياً، لإرغام المسارات على مغادرة مباشرة للمرحلة الصفرية نضع $d(00\cdots0;1) = \infty$. ولهذا نسقط من حساباتنا المسارات التي تبقى عند المرحلة الصفرية؛ لأن المسار المتبقي حيث $d(s;1)$ منته، هو المسار إلى $s = 100\cdots0$ (أي المسار المغادر مباشرة المرحلة الصفرية). ثالثاً، لا نحتاج إلى تخزين المسارات $W(s;t)$؛ لأنها لا تؤثر في هذه الحسابات. رابعاً، يجب علينا معرفة الاجابة! لكل شفرة غير اخفاقية، نرى أن كل مسار من المسارات ذات الوزن المنتهي الذي يعود إلى المرحلة الصفرية يبقى في هذه المرحلة ولا يغادرها أبداً. عند كل تكّة t، تكون $d(s;t)$ هي وزن مسار أصغري من الطول t الذي يغادر مباشرة المرحلة الصفرية وينتهي عند المرحلة s. أيضاً إذا كان $d(s;t) \geq d(00\cdots0;t)$ عند التكّة t لكل المراحل s فنجد أن $d(00\cdots0;t') = d(00\cdots0;t)$ لكل $t' \geq t$ (استناداً إلى الخطوة (٢) من الخوارزمية (٨,٤,١) يكون من الواضح أن $d(s';t') \geq min_s\{d(s;t'-1)\}$ لكل مرحلة s'). إذن، $d(C) = d(00\cdots0;t)$. وبالمثل، بمجرد أن يكون $d(s;t) > 2e$ لكل مرحلة s، نرى أن وزن جميع المسارات من الطول t التي تغادر مباشرة المرحلة الصفرية أكبر من $2e$. وبهذا نجد أن $\tau(e)$ هو أول تكّة t تحقق $d(s;t) > 2e$ لكل مرحلة s. وعليه يكون لدينا التعديل التالي للخوارزمية (٨,٤,١) لحساب $d(C)$ و $\tau(e)$.

خوارزمية (٨,٤,١٢) [إيجاد $d(C)$ و $\tau(e)$ لشفرات تلاف غير إخفاقية]

نفرض أن $wt(s;s')$ وزن الضلع الموجّه من s إلى s' في مخطط المراحل. يتم تنفيذ الخطوات التالية:

(١) إذا كان $t = 1$ فنعرّف:

$$d(s;t) = \begin{cases} wt(00\cdots0;100\cdots0) & ,s = 100\cdots0 \\ \infty & \text{خلاف ذلك}, \end{cases}$$

(٢) لكل $t > 1$ ولكل مرحلة $s = s_0,\cdots,s_{m-1}$ نعرّف:

$$d(s;t) = min\{d(s_0,\cdots,s_{m-1},0;t-1) + wt(s_0,\cdots,s_{m-1},0;s), d(s_0,\cdots,s_{m-1},1;t-1) + wt(s_0,\cdots,s_{m-1},1;s)\}$$

(٣) إذا كان $d(00\cdots0;t) \geq d(s;t)$ لكل مرحلة s فإن $d(C) = d(00\cdots0;t)$.

(٤) إذا كان $d(s;t) > 2e$ لكل مرحلة s وتوجد مرحلة s' حيث $d(s';t-1) \leq 2e$ فإن $\tau(e) = t$.

ملحوظة

إذا فرضنا أن الكلمة المستقبلة هي $w = 000\cdots$ فتكون الخوارزمية (٨,٤,١٢) هي الخوارزمية (٨,٤,١) مع الفرق الوحيد وهو تعريفنا $d(00\cdots00;1) = \infty$ وعدم حساب $W(s;t)$.

مثال (٨,٤,١٣)

نحسب $d(C)$ و $\tau(e)$ حيث $1 \leq e \leq \lfloor(d(C)-1)/2\rfloor$ للشفرة C_1 التي لها المولّدان $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$ (قمنا سابقاً بهذه الحسابات في المثال (٨,٣,٦) والفقرة المقدمة قبل المثال (٨,٣,٥)). سنستخدم المثال (٨,٤,٢) عند تنفيذ الخوارزمية (٨,٤,١).

المرحلة	المخرج											
s	$X_3 = 0$	$X_3 = 1$	$t = 1$	2	3	4	5	6	7	8	9	10
000	00	11	∞	∞	∞	6	6	6	6	6	6	6
100	11	00	2	∞	∞	4	6	4	6	6	6	6
010	10	01	∞	3	∞	5	5	5	5	7	7	7
110	01	10	∞	3	∞	5	5	5	5	7	7	7
001	01	10	∞	∞	4	6	4	6	6	6	6	6
101	10	01	∞	∞	4	6	4	6	6	6	6	6
011	11	00	∞	∞	5	3	5	5	5	5	5	7
111	00	11	∞	∞	3	5	5	5	5	5	7	7

عند $t = 10$: $d(000;10) \geq d(s;10)$ لكل مرحلة s، وبهذا يكون $d(C) = d(000;10) = 6$ (من الخطوة (٣) في الخوارزمية (**٨,٤,١١**)). بما أن $1 \leq e \leq \lfloor (d(C)-1)/2 \rfloor$ فنرى أن $e = 1$ و $e = 2$.

عند $e = 1$: $d(s;2) > 2e$ لكل مرحلة s وإن $d(000;1) = 2 \leq 2e$. إذن، باستخدام الخطوة (٤) من الخوارزمية (**٨,٤,١٢**) يكون $\tau(1) = 2$.

عند $e = 2$: $d(s;7) > 2e$ لكل مرحلة s وإن $d(100;6) = 4 \leq 2e$. إذن، باستخدام الخطوة (٤) من الخوارزمية (**٨,٤,١٢**) نجد أن $\tau(1) = 2$. ▲

تمرين

(**٨,٤,١٤**) لكل من شفرات التلاف C ذات المولّدات المبيّنة، استخدم الخوارزمية (**٨,٤,١٢**) لحساب $d(C)$ و $\tau(e)$ حيث $1 \leq e \leq \lfloor (d(C)-1)/2 \rfloor$. قارن إجابتك مع إجابات التمرينين (**٨,٣,٣**) و (**٨,٣,٦**).

(أ) $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$.

(ب) $g_1(x) = 1 + x + x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$.

(ج) $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

الفصل التاسع

شفرات ريد ومولر وشفرات بريبراتا
Reed-Muller & Preparata Codes

(٩,١) شفرات ريد ومولر
Reed-Muller Codes

قدّمنا في الفصل الثالث طريقة لإنشاء شفرات ريد ومولر $RM(r,m)$ ودرسنا عديداً من خواصها الأساسية. من هذه الخواص، أنها شفرات خطيّة من النوع (n,k,d) حيث $n = 2^m$ ، $k = \sum_{i=1}^{r}\binom{m}{i}$ ، $d = 2^{m-r}$. نقوم في هذا البند بإنشاء هذه الشفرات بطريقة أنسب لعملية فك التشفير.

وكما هو الحال مع شفرات ريد وسولومن والشفرات الأخرى، نقوم بتعليم مواقع إحداثيات الكلمات من الطول $n = 2^m$ ونستخدم هنا متجهات K^m. لغرض الاتّساق والسهولة نقوم بتعليم موقع الإحداثي i بالمتجه $u_i \in K^m$ حيث u_i هو التمثيل الثنائي للعدد الصحيح i ونكتب الإحداثيات بترتيب معكوس (نكتب الإحداثي ذا الترتيب الأصغر أولاً). ونُسمي ذلك، **الترتيب المعتاد (Standard Ordering)** لمتجهات K^m.

مثال (٩,١,١)

الترتيب المعتاد لمتجهات K^2 هو $(00, 10, 01, 11)$ والترتيب المعتاد لمتجهات K^3 هو:

$(000, 100, 010, 110, 001, 101, 011, 111)$. ▲

لكـل دالـة f مـن K^m إلى $\{0,1\}$ يوجـد تمثيـل وحيـد (شـكل متجهـي وحيـد) $v = (f(u_0), f(u_1), \cdots, f(u_{2^m-1}))\epsilon K^m$ حيـث $u_i \epsilon K^m$ ، $n = 2^m$ ، $u_0, u_1, \cdots, u_{2^m-1}$ بالترتيب المعتاد لمتجهات K^m كما هو موصوف في بداية البند.

ينصب اهتمامنا على صنف خاص من الدوال الأساسية. فإذا كانت I مجموعة جزئية من $\{0,1,\cdots,m-1\}$ ، نعرّف الدالة :

$$f_I(x_0, x_1, \cdots, x_{m-1}) = \begin{cases} \prod_{i\epsilon I}(x_i + 1) & , I \neq \phi \\ 1 & , I = \phi \end{cases}$$

(f_I دالة من K^m إلى $\{0,1\}$). نفرض أن v_I هو الشكل المتجهي المقابل للدالة f_I.

مثال (٩,١,٢)

لنفرض أن $m = 3$ ومن ثم فإن $n = 2^3$.

(أ) إذا كانت $I = \{1,2\}$ فنرى أن $f_I(x_0, x_1, x_2) = (x_1 + 1)(x_2 + 1)$. والمتجه المقابل للدالة $f_{\{1,2\}}(x_0, x_1, x_2)$ يمكن إيجاده بأخذ كل عنصر $x_0x_1x_2\epsilon K^3$ من عناصر K^3 (بالترتيب المعتاد) وإيجاد القيمة $f_{\{1,2\}}(x_0, x_1, x_2)$. وبهذا نرى أن :

$$f_{\{1,2\}}(0,0,0) = 1, f_{\{1,2\}}(1,0,0) = 1, f_{\{1,2\}}(0,1,0) = 0, f_{\{1,2\}}(1,1,0) = 0,$$
$$f_{\{1,2\}}(0,0,1) = 0, f_{\{1,2\}}(1,0,1) = 0, f_{\{1,2\}}(0,1,1) = 0, f_{\{1,2\}}(1,1,1) = 0$$

إذن ، $v_I = 11000000$.

(ب) إذا كانت $I = \{0\}$ فنرى أن $f_I(x_0, x_1, x_2) = (x_0 + 1)$ ويكون $v_I = 10101010$.

(ج) إذا كانت $I = \phi$ فنرى أن $f_\phi(x_0, x_1, x_2) = 1$ ويكون $v_I = 11111111$.

▲

سنسـتخدم لاحقـاً الحقيقـتين التـاليتين عـن الدالـة f_I. الأولى هـي أن $f_I(x_0, x_1, \cdots, x_{m-1}) = 1$ إذا وفقط إذا كان $x_i = 0$ لكل $i\epsilon I$.

ففي المثال (٩,١,٢) (أ)، $I = \{1,2\}$ ، $f_I(x_0, x_1, x_2) = (x_1 + 1)(x_2 + 1)$ ومن ثم يكون $f_I(x_0, 0,0) = (0 + 1)(0 + 1) = 1$ لكل $x_0\epsilon\{0,1\}$.

أما الحقيقة الثانية فهي $f_I(u_i)f_J(u_i) = f_{I\cup J}(u_i)$ لكل $u_i \epsilon K^m$. وبهذا يكون:

$$\begin{aligned} v_I \cdot v_J &= \sum_{i=0}^{2^m-1} f_I(u_i)f_J(u_i) \\ &= \sum_{i=0}^{2^m-1} f_{I\cup J}(u_i) \\ &\equiv Wt\left(v_{I\cup J}\right) \ (mod\ 2) \end{aligned}$$

نستخدم الرمز $\mathbb{Z}_m$ للمجموعة $\{0,1,2,\cdots,m-1\}$.

تمارين

(**٩,١,٣**) ليكن $m = 4$ ومن ثم $n = 2^4$. لكل من المجموعات الجزئية $I \subseteq \mathbb{Z}_4$ ، جد f_I و v_I:

(أ) $I = \{0,3\}$ (ب) $I = \{0,1,3\}$

(ج) $I = \{1\}$ (د) $I = \{2,3\}$

(هـ) $I = \phi$ (و) $I = \mathbb{Z}_4$.

(**٩,١,٤**) ليكن $m = 5$ ومن ثم $n = 2^5$. لكل من المجموعات الجزئية $I \subseteq \mathbb{Z}_5$ ، جد f_I و v_I:

(أ) $I = \{0,2,4\}$ (ب) $I = \{0,1,3,4\}$

(ج) $I = \{1\}$ (د) $I = \{1,2,4\}$

(هـ) $I = \phi$ (و) $I = \mathbb{Z}_5$.

(**٩,١,٥**) لتكن $I \subseteq \mathbb{Z}_m$. استخدم الحقيقة الأولى المقدمة في الصفحة السابقة لإثبات أن $wt(v_I) = 2^{m-|I|}$.

(**٩,١,٦**) إذا كان v تركيباً خطياً لمتجهات على الصورة v_I فمتى يكون وزن v زوجياً؟

(**٩,١,٧**) ليكن $m = 4$ ومن ثم $n = 2^4$. إذا كان $I = \{0,1,3\}$ و $J = \{2,3\}$ فاحسب $v_I \cdot v_J$.

من الممكن تعريف شفرة ريد ومولر $RM(r,m)$ على أنها الشفرة الخطيّة $\langle\{v_I: I \subseteq \mathbb{Z}_m, |I| \leq r\}\rangle$.

لاحظ أن المجموعة $S = \{v_I: I \subseteq \mathbb{Z}_m, |I| \leq r\}$ مُستقلة خطياً (انظر التمرين (**٩,١,١٠**)) ومن ثم فهي أساس للشفرة $RM(r,m)$. وبحساب عدد الكلمات v_I حيث $I \subseteq \mathbb{Z}_m$ و $|I| \leq r$ نجد الشفرة $RM(r,m)$ أن:

$$k = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}$$

ومن الواضح أن $n = 2^m$. ومن الواضح أيضاً أنه يمكن ترتيب الكلمات v_I بأي طريقة لتشكيل مصفوفة مولّدة للشفرة $RM(r,m)$. نقول إن مصفوفة مولّدة $G_{r,m}$ للشفرة $RM(r,m)$ على **شكل قانوني** (**Canonical Form**) إذا كانت صفوفها مرتبة بحيث تأتي v_I قبل v_J إذا كان $|I| < |J|$ أو كان $|I| = |J|$ ، $f_I(u_j) < f_J(u_j)$ و $f_I(u_i) = f_J(u_i)$ لكل $i > j$.

مثال (٩,١,٨)

الشكل (**٩,١**) يُبيّن مصفوفة مولّدة $G_{4,4}$ على شكل قانوني للشفرة $R(4,4)$. لسهولة الترميز كتبنا v_3 عوضاً عن $v_{\{3\}}$ (وهكذا لبقية المتجهات). نحصل على الترتيب السابق من التعريف كما تبيّن الأمثلة التالية. إذا كان $I = \{3\}$ و $J = \{2,3\}$ فإن $|I| < |J|$ ومن ثم $v_3 = v_I$ يقع ترتيبه قبل $v_{2,3} = v_J$. وإذا كان $I = \{2,3\}$ و $J = \{0,2\}$ فيكون $f_I(u_j) = f_J(u_j)$ لكل $i > 0$ ولكن $f_I(u_{10}) = 0 < 1 = f_J(u_{10})$ (لاحظ أن الترتيب المعتاد للمتجه $u_{10} \epsilon K^4$ هو 0101). إذن، $v_{2,3} = v_I$ يقع ترتيبه قبل $v_{0,2} = v_J$.

من السهل أن نرى أن $G_{0,4}$ ، $G_{1,4}$ ، $G_{2,4}$ ، $G_{3,4}$ هي المصفوفات الجزئية من $G_{4,4}$ المكوّنة من الصفوف الأولى وعددها $1 = \binom{4}{0}$، $5 = \binom{4}{0} + \binom{4}{1}$، $11 = \binom{4}{0} + \binom{4}{1} + \binom{4}{2}$، $15 = \binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3}$ من صفوف $G_{4,4}$ على التوالي. ▲

$$G_{4,4}=\left[\begin{array}{cccccccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right]
\begin{array}{l}
v_{\emptyset}\\ v_3\\ v_2\\ v_1\\ v_0\\ \\ v_{2,3}\\ v_{1,3}\\ v_{0,3}\\ v_{1,2}\\ v_{0,2}\\ v_{0,1}\\ \\ v_{1,2,3}\\ v_{0,2,3}\\ v_{0,1,3}\\ v_{0,1,2}\\ \\ v_{0,1,2,3}
\end{array}$$

الشكل (٩,١). المصفوفة المولّدة $G_{4,4}$.

تمارين

(٩,١,٩) جد كلاً من $G_{2,3}$ ، $G_{2,4}$ ، $G_{3,5}$ ، $G_{0,10}$.

(٩,١,١٠) أثبت أن المجموعة $\{v_I : |I| \le r, I \subseteq \mathbb{Z}_m\}$ مُستقلة خطياً لكل $r \le m$

[**إرشاد**: رتّب عناصر المجموعة بحيث يأتي v_I قبل v_J إذا وجد j بحيث يكون $f_I(u_j) = f_J(u_j)$ عندما $j + 1 \le i \le m$ ويكون $f_I(u_j) > f_J(u_j)$. أو استخدم الاستقراء على m و r].

تتم عملية التشفير مثل أي تشفير للشفرات الخطيّة حيث نقوم بضرب الرسالة بالمصفوفة $G_{r,m}$. وبهذا تكتب كل من كلمات الشفرة c على النحو التالي :

$$c = \sum_{I \subseteq \mathbb{Z}_m, |I| \leq r} m_I v_I$$

حيث قمنا بتعليم إحداثيات الرسالة m_I لتقابل الصف v_I من المصفوفة $G_{r,m}$.

مثال (٩,١,١١)

عند استخدام $G_{2,4}$ لتشفير الرسائل m نحصل على كلمة الشفرة c المقابلة.

(أ) إذا كانت : $(m_{0,3} = 1, m_\phi = 1) m = 1\ \ 0000\ \ 001000$.

فإن : $c = v_\phi + v_{0,3} = 0101010111111111$.

(ب) : إذا كانت $(m_2 = m_0 = m_{0,3} = m_{0,1} = 1) m = 0\ \ 0101\ \ 001001$.

فإن : $c = v_2 + v_0 + v_{0,3} + v_{0,1} = 0111100011010010$. ▲

تمرين

(**٩,١,١٢**) شفّر كلاً من الرسائل التالية باستخدام المصفوفة $G_{2,4}$:

(أ) $0\ \ 0101\ \ 000000$.

(ب) $0\ \ 0000\ \ 000001$.

(ج) $0\ \ 0100\ \ 001000$.

(٩,٢) فك تشفير شفرات ريد ومولر
Decoding Reed-Muller Codes

نستخدم طريقة سهلة التنفيذ لفك تشفير شفرات ريد ومولر تُدعى **فك التشفير المنطقي الغالب (Majority Logic Decoding)**. ولفهم هذه الطريقة يلزمنا بعض التحضير لذلك. إذا كانت $I \subseteq \mathbb{Z}_m$ فإن $I^c = \mathbb{Z}_m \backslash I$ هي متممة I في المجموعة $\mathbb{Z}_m$. لنفرض أن $H_I = \{u \epsilon K^m : f_I(u) = 1\}$. تذكر أن $f_I(x_0, \cdots, x_{m-1}) = \prod_{i \epsilon I}(x_i + 1) = 1$ إذا وفقط إذا كان $x_i = 0$ لكل $i \epsilon I$. إذا كان $x, y \epsilon H_I$ فمن الواضح أن $x_i = y_i = 0 = x_i + y_i$

لكل $i\epsilon I$، ومن ذلك نرى أن $x+y\epsilon H_I$. وبهذا يكون H_I فضاءً جزئياً من K^m. لكل $u=(x_0,\cdots,x_{m-1})\epsilon K^m$ ولكل $t=(t_0,t_1,\cdots,t_{m-1})\epsilon K^m$ نعرّف الدالة:

$$f_{I,t}(x_0,x_1\cdots,x_{m-1})=f_I(x_0+t_0\cdots,x_{m-1}+t_{m-1})=f_I(x+t)$$

ونعرّف $v_{I,t}$ على أنه الشكل المتجهي المقابل للدالة $f_{I,t}$.

سيكون اهتمامنا منصباً على إيجاد $v_{I,s}\cdot v_{J^c,t}$. ولهذا نحتاج إلى حساب عدد الكلمات $u\epsilon K^m$ التي تحقق $f_{I,s}(u)f_{J^c,t}(u)=1$. من تعريف H_I نرى أن $f_{I,t}(u)=f_I(u+t)=1$ إذا وفقط إذا كان $u+t=u'\epsilon H_I$ أو بصورة مكافئة $u=u'+t\epsilon H_I+t$ حيث H_I+t هي مجموعة H_I المشاركة التي يحددها t. كما أن القيمة $f_{I,s}(u)f_{J^c,t}(u)=\prod_{i\epsilon I}(x_i+s_i+1)\prod_{j\epsilon J^c}(x_j+t_j+1)$ لا تتغير لكل $x_k\epsilon\{0,1\}$، $k\epsilon\mathbb{Z}_m\backslash(I\cup J^c)$. وبما أنه يوجد $2^{m-|I\cup J^c|}$ خياراً للعناصر $u\epsilon K^m$ فنرى أن عدد المرات التي يكون فيها:

$$f_{I,s}(u)f_{J^c,t}(u)=1$$

هو مضاعف للعدد $2^{m-|I\cup J^c|}$ وهذا عدد زوجي ما عدا الحالة $|I\cup J^c|=m$. أي ما عدا الحالة $|I\cup J^c|=\mathbb{Z}_m$ وأما إذا فرضنا أن $|J|\leq|I|$ فنرى أن $|J^c|\leq|I^c|$ ومن ثم يكون $|I\cup J^c|=|I|+|J^c|-|I\cap J^c|<m$ إلاّ إذا كان $I=J$. وإذا كان $I=J$ فيوجد عنصر واحد $u\epsilon K^m$ يحقق $f_{I,s}(u)f_{I^c,t}(u)=1$ ، بالتحديد هذا العنصر u هو العنصر الذي يكون فيه $x_i=s_i$ لكل $i\epsilon I$ و $x_i=t_i$ لكل $i\epsilon I^c$. وبما أن إيجاد عدد المواقع التي يكون فيها $f_{I,s}(u)f_{J^c,t}(u)=1$ يُعطي مباشرة $v_{I,s}\cdot v_{J^c,t}$ فنكون قد برهنا التمهيدية التالية:

تمهيدية (٩,٢,١)

لتكن كل من I و J مجموعة جزئية من$\mathbb{Z}_m$ حيث $|J|\leq|I|$. لكل $s\epsilon H_{I^c}$ ولكل $t\epsilon H_J$ لدينا:

$$v_{I,s}\cdot v_{J^c,t}=1$$ إذا وفقط إذا كان $I=J$.

نستطيع الآن وبسهولة الحصول على النتيجة التالية التي تعد الركيزة الأساسية لخطة فك التشفير التي سنستخدمها لاحقاً.

نتيجة (٩,٢,٢)

إذا كانت $c\epsilon RM(r,m)$ كلمة شفرة وكان $|J| = r$ فإن $m_J = c \cdot v_{J^c,t}$ لكل $t\epsilon H_J$.

البرهان

إذا كان $|J| = r$ فلكل $t\epsilon H_J$ نجد أن :

$$c \cdot v_{J^c,t} = \sum_{I\subseteq \mathbb{Z}_m, |I| \le r} m_I v_I \cdot v_{J^c,t} = m_J v_J \cdot v_{J^c,t} = m_J$$

وذلك لأنه استناداً إلى التمهيدية (٩,٢,١) يكون الضرب القياسي الوحيد الذي لا يساوي صفراً في هذا المجموع هو الضرب الذي يحقق $I = J$. ■

تمهيدية (٩,٢,٣)

لتكن $J \subseteq \mathbb{Z}_m$. لكل كلمة e من الطول 2^m يكون $e \cdot v_{J^c,t} = 1$ لعلى الأكثر $wt(e)$ قيمة من القيم $t\epsilon H_J$.

البرهان

تذكر أنه لأي فضاء جزئي S من K^m تنتمي كلمتان إلى مجموعة مشاركة واحدة من المجموعات المشاركة لـ S إذا وفقط إذا كان مجموع الكلمتين كلمة تنتمي إلى S. كما أن H_J فضاء جزئي من K^m وأن $H_J \cap H_{J^c} = \{0\}$. من ذلك نرى عدم وجود كلمتين من كلمات H_J تنتميان إلى مجموعة مشاركة واحدة لـ H_{J^c}. وبهذا تكون $H_{J^c} + t$ هي جميع المجموعات المشاركة لـ H_{J^c} حيث t مأخوذة على جميع عناصر H_J. نحصل الآن على المطلوب بملاحظة أنه إذا كان $t_1, t_2 \epsilon H_J$ حيث $t_1 \neq t_2$ فإن $(H_{J^c} + t_1) \cap (H_{J^c} + t_2) = \phi$ ومن ثم لا يوجد موقع مشترك بين v_{J^c,t_1} و v_{J^c,t_2} بحيث يكون الإحداثيان 1. إذن، كل

من الإحداثيات $wt(e)$ غير الصفرية في e تؤثر على قيمة واحدة على الأكثر من القيم $e \cdot v_{J^c,t}$ حيث t مأخوذة على جميع عناصر H_J. ■

نحصل الآن على خوارزمية فك تشفير على النحو التالي:

نفرض أن $w = c + e$ هي الكلمة المستقبلة حيث c كلمة شفرة تنتمي إلى $RM(r, m)$. عندئذ، $c = \sum_{I \subseteq \mathbb{Z}_m, |I| \le r} m_I v_I$ حيث $|I| \le r$. لنفرض أن $J \subseteq \mathbb{Z}_m$ حيث $|J| = r$. استناداً إلى التمهيدية (**٩,٢,٣**)، نرى أن $e \cdot v_{J^c,t} = 0$ لعلى الأقل $|H_J| - wt(e)$ قيمة من قيم $t \epsilon H_J$.

لكل قيمة t من هذه القيم لدينا:

$$\begin{aligned} w \cdot v_{J^c,t} &= c \cdot v_{J^c,t} + e \cdot v_{J^c,t} \\ &= c \cdot v_{J^c,t} \\ &= m_J \end{aligned}$$

(باستخدام النتيجة (**٩,٢,٢**)).

وبهذا، إذا كان $2wt(e) < |H_J|$ حيث مجال t هو عناصر H_J فنرى أن أكثر من نصف القيم $w \cdot v_{J^c,t}$ يكون m_J. وبمجرد الانتهاء من حساب m_J بهذه الطريقة لكل $J \subseteq I_m$ حيث $|J| = r$، نضع $w(r-1) = w + \sum_{|J|=r} m_J v_J$. الآن، يمكن فك تشفير $w(r-1)$ على اعتبار أنها الكلمة المستقبلة التي تم تشفيرها باستخدام الشفرة $RM(r-1, m)$. ونستمر بهذا الأسلوب حتى ننتهي من إيجاد m_J لجميع $J \subseteq I_m$ حيث $|J| \le r$.

قبل تقديم وصف لهذه الخوارزمية، لاحظ أن هذه الخوارزمية تصوّب جميع أنماط الأخطاء التي وزنها أصغر من $|H_J|/2$ حيث $|J| \le r$. ولكن باستخدام التمرين (**٩,١,٥**)، نعلم أن $|H_J| = wt(v_J) = 2^{m-|J|}$. إذن، يتم تصويب جميع أنماط الأخطاء التي وزنها أصغر من 2^{m-r-1} وبهذا تكون مسافة الشفرة $RM(r, m)$ هي على الأقل 2^{m-r}.

ومن ناحية أخرى، إذا كانت $I \subseteq \mathbb{Z}_m$ و $|I| = r$ فنرى أن v_I كلمة من كلمات الشفرة $RM(r, m)$ وزنها يساوي 2^{m-r}.

وبهذا نكون قد قدّمنا برهاناً آخر للنتيجة التالية:

تمهيدية (٩,٢,٤)

مسافة الشفرة $RM(r, m)$ تساوي 2^{m-r}.

خوارزمية (٩,٢,٥) [فك التشفير المنطقي الغالب للشفرة $RM(r,m)$]

نفّذ الخطوات التالية لفك تشفير كلمة مستقبلة:

(١) ضع $i = r$ و $w(r) = w$.

(٢) لكل $J \subseteq \mathbb{Z}_m$ حيث $|J| = i$، احسب $w(i) \cdot v_{J^c,t}$ لكل $t \epsilon H_J$ حتى يظهر الإحداثي 0 أو الإحداثي 1 أكثر من 2^{m-i-1} مرة ومن ثم ضع $m_J = 0$ أو $m_J = 1$ على التوالي. إذا ظهر كل من الإحداثيين 0 و 1 أكثر من $e = 2^{m-r-1} - 1$ مرة فاطلب إعادة إرسال.

(٣) إذا كان $i > 0$ فضع $w(i-1) = w(i) + \sum_{J \subseteq \mathbb{Z}_m} m_J v_J$ حيث $|J| = i$. إذا كان وزن $w(i-1)$ على الأكثر $e = 2^{m-r-1} - 1$ فضع $m_J = 0$ لكل $J \subseteq \mathbb{Z}_m$ حيث $r \geq |J|$ وتوقف. وإذا لم يتحقق ذلك استبدل i بالعدد $i - 1$ وارجع إلى الخطوة (٢). (إذا كان $i = 0$ فنكون قد حسبنا m_J لكل $J \subseteq \mathbb{Z}_m$ حيث $|J| \leq r$ ومن ثم نكون قد وجدنا الرسالة المرجحة).

مثال (٩,٢,٦)

استخدم الخوارزمية (٩,٢,٥) لفك تشفير الكلمة المستقبلة $w = 0101011110100000$ التي سبق وشُفّرت باستخدام $G_{4,4}$.

الحل

ابـدأ بوضـع $i = r = 2$ و $w = w(2)$. مـن حسـابات الشـكل (**٩,٢**) نـرى أن $m_{2,3} = 0$ ، $m_{1,3} = 0$ ، $m_{0,3} = 0$ ، $m_{1,2} = 0$ ، $m_{0,2} = 1$ ، $m_{0,1} = 0$. إذن $w(1) = w(2) + v_{0,2} = 1111\ 0111\ 0000\ 0000$ ويكون $i = 1$.

J	t	$v_{J^c,t}$	$w \cdot v_{J^c,t}$	m_J
{0,1}	0000	1111 0000 0000 0000	0	
	0010	0000 1111 0000 0000	1	0
	0001	0000 0000 1111 0000	0	
	0011	0000 0000 0000 1111	0	
{0,2}	0000	1100 1100 0000 0000	0	
	0100	0011 0011 0000 0000	1	1
	0001	0000 0000 1100 1100	1	
	0101	0000 0000 0011 0011	1	
{1,2}	0000	1010 1010 0000 0000	1	
	1000	0101 0101 0000 0000	0	0
	0001	0000 0000 1010 1010	0	
	1001	0000 0000 0101 0101	0	
{0,3}	0000	1100 0000 1100 0000	0	
	0100	0011 0000 0011 0000	0	0
	0010	0000 1100 0000 1100	1	
	0110	0000 0011 0000 0011	0	
{1,3}	0000	1010 0000 1010 0000	0	
	1000	0101 0000 0101 0000	0	0
	0010	0000 1010 0000 1010	1	
	1010	0000 0101 0000 0101	0	
{2,3}	0000	1000 1000 1000 1000	1	
	1000	0100 0100 0100 0100	0	0
	0100	0010 0010 0010 0010	0	
	1100	0001 0001 0001 0001	0	

الشكل (٩,٢). فك التشفير المنطقي للشفرة $RM(2,4)$ (الخطوة ١).

مرة أخرى، نرى من حسابات الشكل (**٩,٣**) أن $m_3 = 1$ ، $m_2 = 0$ ، $m_1 = 0$ ، $m_0 = 0$. ضع $w(0) = w(1) - v_3 = 0000\ 1000\ 0000\ 0000$ وضع $i = 0$. بما أن وزن $w(0)$

على الأكثر هو $e = 1$ فنضع $m_\phi = 0$ ونتوقف. إذن، الرسالة المرجحة هي 0 1000 000010 0 (شُفِّرت الرسائل باستخدام $G_{2,4}$). ▲

J	t	$v_{J^c,t}$	$w_{(1)} \cdot v_{J^c,t}$	m_J
{0}	0000	1100 0000 0000 0000	0	
	0100	0011 0000 0000 0000	0	
	0010	0000 1100 0000 0000	1	0
	0110	0000 0011 0000 0000	0	
	0001	0000 0000 1100 0000	0	
	0101	0000 0000 0011 0000	0	
	0011	0000 0000 0000 1100		
	0111	0000 0000 0000 0011		
{1}	0000	1010 0000 0000 0000	0	
	1000	0101 0000 0000 0000	0	
	0010	0000 1010 0000 0000	1	0
	1010	0000 0101 0000 0000	0	
	0001	0000 0000 1010 0000	0	
	1001	0000 0000 0101 0000	0	
	0011	0000 0000 0000 1010		
	1011	0000 0000 0000 0101		
{2}	0000	1000 1000 0000 0000	1	
	1000	0100 0100 0000 0000	0	
	0100	0010 0010 0000 0000	0	0
	1100	0001 0001 0000 0000	0	
	0001	0000 0000 1000 1000	0	
	1001	0000 0000 0100 0100	0	
	0101	0000 0000 0010 0010		
	1101	0000 0000 0001 0001		
{3}	0000	1000 0000 1000 0000	1	
	1000	0100 0000 0100 0000	1	
	0100	0010 0000 0010 0000	1	1
	1100	0001 0000 0001 0000	1	
	0010	0000 1000 0000 1000	0	
	1010	0000 0100 0000 0100	1	
	0110	0000 0010 0000 0010		
	1110	0000 0001 0000 0001	1	

الشكل (٩,٣). فك التشفير المنطقي للشفرة $RM(2,4)$ (الخطوة ٢).

تمارين

(**٩,٢,٧**) إذا علمت أن الرسائل شُفِّرت باستخدام المصفوفة $G_{2,4}$ ففك تشفير الكلمات المستقبلة التالية إن أمكن ذلك.

(أ) $w = 0111\ 0101\ 1000\ 1000$

(ب) $w = 0110\ 0110\ 0001\ 0000$

(ج) $w = 0101\ 1010\ 0100\ 0101$

(د) $w = 1110\ 1000\ 1001\ 0001$

(هـ) $w = 0011\ 0000\ 0011\ 0100$

(و) $w = 1001\ 0110\ 0101\ 1010$

(ز) $w = 1010\ 1000\ 1010\ 0000$

(ح) $w = 0011\ 1100\ 0001\ 1100$

(ط) $w = 1001\ 1101\ 0001\ 1101$

(**٩,٢,٨**) إذا علمت أن الرسائل شُفِّرت باستخدام المصفوفة $G_{2,4}$ ففك تشفير الكلمات المستقبلة التالية إن أمكن ذلك.

(أ) $w = 1100\ 1000\ 1110\ 0000\ 1100\ 0000\ 1100\ 0100$.

(ب) $w = 0101\ 0111\ 0101\ 1000\ 1000\ 1000\ 0111\ 1010$.

(ج) $w = 0011\ 0011\ 1111\ 0011\ 0011\ 0011\ 1111\ 1111$.

(د) $w = 0100\ 0000\ 1111\ 1111\ 0000\ 1100\ 0000\ 1111$.

(هـ) $w = 1001\ 0101\ 0110\ 1001\ 1001\ 0111\ 0110\ 1010$.

(و) $w = 0011\ 1111\ 0011\ 0011\ 1100\ 1100\ 1100\ 0100$.

(ز) $w = 0100\ 0100\ 1111\ 1111\ 0000\ 1100\ 0000\ 1111$.

(٩,٣) شفرات بريبراتا الممتدة
Extended Preparata Codes

في هذا البند نقوم بتعليم إحداثيات مواقع الكلمات من الطول 2^r باستخدام عناصر الحقل $GF(2^r)$. لقد سبق وأن استخدمنا طريقة التعليم هذه عند دراستنا لشفرات BCH حيث استخدمنا جميع كلمات الحقل غير الصفرية للتعليم. فإذا كانت U مجموعة جزئية من الحقل $GF(2^r)$ فنعرّف الكلمة $\chi(U)$ من الطول 2^r على النحو التالي:

نضع 1 في الموقع i إذا كان $\beta^i \epsilon U$ لكل $0 \le i \le 2^r - 2$.

نضع 1 في الموقع $2^r - 1$ إذا كان $0 \epsilon U$.

نضع 0 في ما تبقى من المواقع. (β عنصر بدائي في الحقل $GF(2^r)$).

مثال (٩,٣,١)

إذا كان β عنصراً بدائياً في الحقل $GF(2^3)$ فيكون:

$$\chi(\{0\}) = 00000001$$
$$\chi(\{\beta^2, \beta^5, \beta^6\}) = 00100110$$
$$.\chi(\phi) = 00000000$$ ▲

لنفرض أن $\alpha \in GF(2^r)$ وأن $U \subseteq GF(2^r)$. نعرّف المجموعتين $U + \alpha$ و αU على أنهما:

$$U + \alpha = \{u + \alpha : u \epsilon U\}$$
$$.\alpha U = \{\alpha u : u \epsilon U\}$$

كما نعرّف **الفرق التناظري (Symmetric Difference)** لمجموعتين جزئيتين U و V من الحقل $GF(2^r)$ ونرمز لذلك بالرمز $U \Delta V$ على النحو التالي:

$$.U \Delta V = \{x : x \epsilon U \cup V, x \notin U \cap V\} = (U \cup V) - (U \cap V)$$

من السهل أن نرى أن:

$$.\chi(U) + \chi(V) = \chi(U \Delta V)$$

مثال (٩,٣,٢)

ليكن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $x^3 + x + 1$. ولتكن $U = \{\beta^2, \beta^5, \beta^6\}$ و $V = \{\beta^2, 0\}$. عندئذ، يكون:

$$U + \beta^2 = \{\beta^2 + \beta^2, \beta^5 + \beta^2, \beta^6 + \beta^2\} = \{0, \beta^3, \beta^0\}$$
$$\beta^2 U = \{\beta^2\beta^2, \beta^2\beta^5, \beta^2\beta^6\} = \{\beta^4, \beta^0, \beta\}$$
$$\begin{aligned}(U) + \chi(V) &= 00100110 + 00000101 \\ &= 00100011 \\ &= \chi(\{\beta^2, \beta^6, 0\}) \\ &= \chi(U \Delta V)\end{aligned}$$
▲

تعريف (٩,٣,٣)

تُعرف شفرة **بريبراتا الممتدة** **(Extended Preparata Code)** $P(r)$ على أنها مجموعة كلمات شفرة على الشكل $\chi(U)$ متبوعة بكلمات شفرة على الشكل $\chi(V)$ حيث U و V مجموعتان جزئيتان من الحقل $GF(2^r)$ بحيث يتحقق ما يلي:

(i) كل من $|U|$ و $|V|$ عدد زوجي.

(ii) $\sum_{u \epsilon U} u = \sum_{v \epsilon V} v$.

(iii) $\sum_{u \epsilon U} u^3 + (\sum_{u \epsilon U} u)^3 = \sum_{v \epsilon V} v^3$.

(iv) r عدد فردي.

نكتب كلمات الشفرة على الصورة $[\chi(U), \chi(V)]$. وبما أن طول كل من $\chi(U)$ و $\chi(V)$ هو 2^r فنرى أن $P(r)$ شفرة طولها 2^{r+1}.

مثال (٩,٣,٤)

ليكن $GF(2^3)$ الحقل المنشأ باستخدام كثيرة الحدود $x^3 + x + 1$. ولنفرض أن $U = \{\beta, \beta^2, \beta^5, 0\}$ و $V = \{\beta^0, \beta, \beta^2, \beta^3, \beta^6, 0\}$. من الواضح أن الشرطين (i) و (iv) من التعريف (**٩,٣,٣**) محققان. أيضاً:

$$\sum_{u\epsilon U} u = \beta + \beta^2 + \beta^5 + 0 = 010 + 001 + 111 + 000 = \beta^0 .$$

$$\sum_{v\epsilon V} v = \beta^0 + \beta + \beta^2 + \beta^3 + \beta^6 + 0 = 100 + 010 + 001 + 110 + 101 + 000 = \beta^0 .$$

ومن ثم فالشرط (ii) محقق. كما أن :

$$\sum_{u\epsilon U} u^3 = \beta^3 + \beta^6 + \beta + 0 = 110 + 101 + 010 + 000 = \beta^2 .$$

$$\sum_{u\epsilon V} v^3 = \beta^0 + \beta^3 + \beta^6 + \beta^2 + \beta^4 + 0 = 100 + 110 + 101 + 001 + 000 = \beta^6$$

ومن ثم فالشرط (iii) محقق ؛ لأن $\beta^2 + (\beta^0)^3 = \beta^6$. إذن ،

$[\chi(U), \chi(V)] = 0110010111110011$ كلمة من كلمات الشفرة $P(3)$. ▲

لاحظ أن وجود (أو عدم وجود) العنصر 0 في المجموعة U أو المجموعة V لا يؤثر في حسابات الشروط (ii)، (iii)، (iv) من التعريف (**٩,٣,٣**). ولهذا فالاستخدام الوحيد للعنصر 0 في V هو جعل $|U|$ أو $|V|$ زوجياً. وبهذا نرى أن الإحداثي الذي في الموقع 2^{r-1} من $\chi(U)$ هو إحداثي اختبار نوعية $\chi(U)$، وبالمثل، الإحداثي الذي في الموقع 2^{r-1} من $\chi(V)$ هو إحداثي اختبار نوعية $\chi(V)$.

سنبيّن في المبرهنة (**٩,٣,١٨**) أن $P(r)$ ليست شفرة خطيّة وبهذا لا يوجد لها بُعد.

تمهيدية (٩,٣,٥)

لتكن كل من $[\chi(U), \chi(V)]$ و $[\chi(A), \chi(B)]$ كلمة شفرة تنتمي للشفرة $P(r)$. ولنفرض أن $\alpha = \sum_{u\epsilon U} u$. عندئذ، $[\chi(U\Delta A + \alpha), \chi(V\Delta B)]$ كلمة شفرة تنتمي إلى $P(r)$.

البرهان

سنثبت أن $[\chi(U\Delta A + \alpha), \chi(V\Delta B)]$ تحقق الشروط (i)، (ii)، (iii) من التعريف (**٩,٣,٣**).

(i) بما أن كل من $|U|$ ، $|V|$ ، $|A|$ ، $|B|$ عدد زوجي فنرى أن :

$$|V\Delta B| = |V| + |B| - 2|V \cap B|$$

وهذا عدد زوجي. كما أن :

$$|U\Delta A + \alpha| = |U\Delta A| = |U| + |A| - 2|U \cap A|$$

وهذا أيضاً عدد زوجي (استخدمنا المثال (**٩,٣,٢**) في المساواة الأولى).

(ii) لاحظ أولاً أن $\sum_{x\epsilon I\Delta J} x = \sum_{x\epsilon I} x + \sum_{x\epsilon J} x$ لكل $I,J \subseteq GF(2^r)$ ؛ وذلك لأن أي $\beta^i \epsilon I \cap J$ يُحسب مرتين في الطرف الأيمن ولا يُحسب في الطرف الأيسر وأن $2\beta^i = 0$.

وبهذا نرى أن :

$$\sum_{x\epsilon U\Delta A+\alpha} x = \sum_{y\epsilon U\Delta A} (y+\alpha) = \sum_{y\epsilon U\Delta A} y + \alpha|U\Delta A|$$

$$= \sum_{y\epsilon U} y + \sum_{y\epsilon A} y + 0 \qquad \text{(لأن } |U\Delta A| \text{ زوجي)}$$

$$= \sum_{y\epsilon V} y + \sum_{y\epsilon B} y$$

$$= \sum_{y\epsilon V\Delta B} y$$

(iii)

$$\sum_{u\epsilon U} x^3 + \left(\sum_{x\epsilon U\Delta A+\alpha} x\right)^3 = \sum_{y\epsilon U\Delta A} (y+\alpha)^3 + \left(\sum_{y\epsilon V\Delta B} y\right)^3$$

$$= \sum_{y\epsilon U} (y+\alpha)^3 + \sum_{y\epsilon A} (y+\alpha)^3 + \left(\sum_{y\epsilon V} y + \sum_{y\epsilon B} y\right)^3$$

$$= \sum_{y\epsilon U} y^3 + \alpha \sum_{y\epsilon U} y^2 + \alpha^2 \sum_{y\epsilon U} y + \alpha^3|U| + \sum_{y\epsilon A} y^3 + \alpha \sum_{y\epsilon A} y^2 + \alpha^2 \sum_{y\epsilon A} y + \alpha^3|A|$$
$$+ \left(\sum_{y\epsilon V} y\right)^3 + \left(\sum_{y\epsilon V} y\right)^2 \left(\sum_{y\epsilon B} y\right) + \left(\sum_{y\epsilon V} y\right)\left(\sum_{y\epsilon B} y\right)^2$$
$$+ \left(\sum_{y\epsilon B} y\right)^3$$

ولكن $\alpha = \sum_{y \epsilon U} y$ ومن ثم $\sum_{y \epsilon V} y = \sum_{y \epsilon U} y = \alpha$. أيضاً، $\left(\sum_{y \epsilon V} y\right)^2 = \sum_{y \epsilon V} y^2$ حيث استخدمنا مرة أخرى حقيقة كون كل من $|U|$ و $|A|$ عدداً زوجياً. وبهذا يختصر المقدار السابق إلى:

$$\sum_{y \epsilon V} y^3 + \sum_{y \epsilon B} y^3 = \sum_{y \epsilon V \Delta B} y^3 \qquad \blacksquare$$

على الرغم من أن الشفرة $P(r)$ ليست خطيّة، إلاّ أنها تشترك مع الشفرات الخطيّة ببعض الخصائص.

تعريف (٩,٣,٦)

نقول عن شفرة C إنها **لا متغيرة المسافة (Distance Invariant)** إذا حققت ما يلي:

لكل $c_1, c_2 \epsilon C$، عدد كلمات الشفرة التي تبعد مسافة i ، $1 \leq i \leq n$، عن c_1 يساوي عدد كلمات الشفرة التي تبعد مسافة i، عن c_2.

من التعريف (٩,٣,٦)، نرى أن مسافة شفرة لا متغيرة المسافة وتحتوي الكلمة الصفرية هي أصغر أوزان كلمات الشفرة غير الصفرية. أي أن:

$.d(C) = min\{wt(c): 0 \neq c \epsilon C\}$

نتيجة (٩,٣,٧)

$P(r)$ شفرة لا متغيرة المسافة.

البرهان

لنفرض أن $[\chi(U), \chi(V)]$ و $[\chi(A), \chi(B)]$ كلمتا شفرة تنتميان إلى $P(r)$ حيث المسافة بينهما تساوي i. استناداً إلى التمهيدية (٩,٣,٥) نرى أن كلاً من $[\chi(U \Delta U + \alpha), \chi(V \Delta V)]$ و $[\chi(U \Delta A + \alpha), \chi(V \Delta B)]$ كلمة شفرة وأنه ليس صعباً أن نرى أن المسافة بينهما تساوي i. بما أن $U \Delta U = \phi$ فنجد أن $[\chi(U \Delta U + \alpha), \chi(V \Delta V)]$ هي الكلمة الصفرية. وبهذا يكون وزن الكلمة $[\chi(U \Delta A + \alpha), \chi(V \Delta B)]$ يساوي i. $\blacksquare$

تقدم التمهيدية التالية بعض خصائص الشفرة $P(r)$ وبرهان هذه الخصائص يشبه البرهان المقدم في التمهيدية (٩,٣,٥)، ولذا نتركه للقارئ.

تمهيدية (٩,٣,٨)

لنفرض أن $[\chi(U),\chi(V)]\epsilon P(r)$. عندئذ، جميع كلمات الشفرة التالية تنتمي إلى $P(r)$:

(i) $[\chi(V),\chi(U)]$.

(ii) $[\chi(U+\alpha),\chi(V+\alpha)]$ لكل $\alpha\epsilon GF(2^r)$.

(iii) $[\chi(\alpha U),\chi(\alpha V)]$ لكل $0\neq\alpha\epsilon GF(2^r)$.

مثال (٩,٣,٩)

إذا كانت $U=\{\beta,\beta^2,\beta^5,0\}$ و $V=\{\beta^0,\beta,\beta^2,\beta^3,\beta^6,0\}$ فقد وجدنا في المثال (٩,٣,٤) أن $[\chi(U),\chi(V)]\epsilon P(3)$. وباستخدام التمهيدية (٩,٣,٨) حيث $\alpha=\beta^3$ نرى أن الكلمات التالية هي كلمات شفرة:

(i) $[\chi(V),\chi(U)]=11110011\ \ 01100101$

(ii) $[\chi(U+\alpha),\chi(V+\alpha)]=[\chi(\{\beta^0,\beta^5,\beta^2,\beta^3\}),\chi(\{\beta,\beta^0,\beta^5,0,\beta^4,\beta^3\})]$
$=10110100\ \ 11011101$

(iii) $[\chi(\alpha U),X(\alpha V)]=[\chi(\{\beta^4,\beta^5,\beta,0\}),\chi(\{\beta^3,\beta^4,\beta^5,\beta^6,\beta^2,0\})]$
$=01001101\ \ 00111111$ ▲

تمارين

(٩,٣,١٠) طبّق التمهيدية (٩,٣,٨) على كلمة الشفرة $[\chi(U),\chi(V)]$ المعرّفة في المثال (٩,٣,٩) في الحالات التالية:

(أ) $\alpha=\beta^0$ (ب) $\alpha=\beta$ (ج) $\alpha=\beta^6$.

(٩,٣,١١) إذا كان $\alpha=0$ فبيّن أن الكلمة $[\chi(\alpha U),\chi(\alpha V)]$ ليست كلمة شفرة (استُثنيت هذه الحالة في التمهيدية (٩,٣,٨)).

(**٩,٣,١٢**) أثبت أن الكلمات التي كوّناها في المثال (**٩,٣,٩**) تحقق التعريف (**٩,٣,٦**).

من الممكن استخدام التمهيدية (**٩,٣,٨**) لتبسيط مسألة إيجاد مسافة الشفرة $P(r)$ ولكن قبل ذلك نقدم التمهيدية التالية التي توضح السبب وراء كون العدد r فردياً.

تمهيدية (٩,٣,١٣)

إذا كان $\beta \epsilon GF(2^r)$ عنصراً بدائياً فإن β^3 عنصر بدائي عندما يكون r فردياً ولكنه ليس عنصراً بدائياً عندما يكون r زوجياً.

البرهان

لاحظ أن β^i عنصر بدائي إذا وفقط إذا كان $gcd(i, 2^r - 1) = 1$ (انظر التمرين (**٥,١,١٨**)).

من السهل أن نبرهن بالاستقراء الرياضي أن:

$$.2^r - 1 \equiv \begin{cases} 1(mod\ 3) & ,\text{فردي } r \\ 0(mod\ 3) & ,\text{زوجي } r \end{cases}$$

أي أن:

$$.2^r - 1 \equiv \begin{cases} 3x + 1 & ,\text{فردي } r \\ 3x & ,\text{زوجي } r \end{cases}$$

وبهذا نرى أن β^3 عنصر بدائي عندما يكون r فردياً ولكنه ليس عنصراً بدائياً عندما يكون r زوجياً. ■

نتيجة (٩,٣,١٤)

إذا كان r عدداً فردياً فلكل عنصر $0 \neq x \epsilon GF(2^r)$ يوجد عنصر وحيد y (الجذر التكعيبي للعنصر x) يحقق $y^3 = x$.

مبرهنة (٩,٣,١٥)

مسافة الشفرة $P(r)$ تساوي 6.

البرهان

بما أن $P(r)$ شفرة لا متغيرة المسافة فنرى أنها تحتوي على كلمة شفرة وزنها d ولتكن كلمة الشفرة هذه هي $[\chi(U),\chi(V)]$. عندئذ،

$$d = wt\left(\chi(U)\right) + wt\left(\chi(V)\right) = |U| + |V|.$$

واستناداً إلى الفقرة (i) من التعريف (**٩,٣,٣**) نرى أن d عدد زوجي. وبهذا يكفي أن نبرهن أن $d \neq 2$ ، $d \neq 4$ وأن $P(r)$ تحتوي على كلمة وزنها 6.

لنفرض أن $d = 2$. عندئذ، استناداً إلى التمهيدية (**٩,٣,٨**) (i)، من الممكن افتراض أن $|U| = 2$ وأن $|V| = 0$. واستناداً إلى التمهيدية (**٩,٣,٨**) (ii)، من الممكن افتراض أن $U = \{0, x\}$ حيث $0 \neq x\epsilon K^r$. وبهذا نرى أن $\sum_{u\epsilon U} u = 0 + x = x$ وهذا يناقض الشرط (ii) من التعريف (**٩,٣,٣**) لأن $V = \phi$.

لنفرض الآن أن $d = 4$. مرة أخرى باستخدام الفقرة (i) من التمهيدية (**٩,٣,٨**) نستطيع افتراض أن ($|U| = 4$ و $|V| = 0$) أو ($|U| = |V| = 2$).

إذا كان $|U| = 4$ و $|V| = 0$ فنرى استناداً إلى الفقرة (ii) من التمهيدية (**٩,٣,٨**) أن $U = \{0, x, y, z\}$ حيث x ، y ، z عناصر غير صفرية مختلفة تنتمي إلى K^4. عندئذ، نجد باستخدام الشرط (iii) من التعريف (**٩,٣,٣**) أن:

$$0^3 + x^3 + y^3 + z^3 + (0 + x + y + z)^3 = 0$$

ومن ذلك يكون $(x + y)(x + z)(y + z) = 0$ وهذا مستحيل لأن x ، y ، z عناصر غير صفرية مختلفة.

وإذا كان $|U| = |V| = 2$ فنستطيع أن نفرض أن $U = \{0, x\}$ ، $V = \{y, z\}$ حيث $y \neq z$. وبتطبيق الشرط (iii) من التعريف (**٩,٣,٣**) نحصل على:

$$0^3 + x^3 + (0 + x)^3 = y^3 + z^3$$

ولكن إذا كان $y^3 = z^3$ فنرى باستخدام النتيجة (**٩,٣,١٤**) أن $y = z$ وهذا تناقض. نجد الآن كلمة شفرة طولها 6. لتكن x ، y ، z عناصر غير صفرية مختلفة من K^r، نفرض أن $w \epsilon K^r$ هو العنصر الوحيد الذي يحقق $w^3 = x^3 + y^3 + z^3$ (استخدمنا النتيجة (**٩,٣,١٤**)). بوضع $u = w + x + y + z$ نرى أن w لا يساوي أياً من x أو y أو z (إذا كان $w = x$ على سبيل المثال، فيكون $w^3 = x^3$ ومن ثم $y^3 + z^3 = 0$ وبهذا نحصل على التناقض $y = z$) وأن $u \neq 0$ (لأن $w^3 + (x + y + z) = (x + y)(x + z)(y + z) \neq 0$ ومن ثم فإن $w \neq x + y + z$). الآن نفرض أن $U = \{0, u\}$ وأن $V = \{w, x, y, z\}$. بما أن $u \neq 0$ وأن $w \neq x \neq y \neq z$ فنرى أن $[\chi(U), \chi(V)]$ كلمة وزنها 6 ومن السهل أن نرى أنها كلمة من كلمات الشفرة $P(r)$. ■

مثال (٩,٣,١٦)

لنفرض أن K^3 هو الحقل المقدم في المثال (**٩,٣,٤**). باستخدام ترميز المبرهنة (**٩,٣,١٥**)، نفرض أن x ، y ، z عناصر غير صفرية مختلفة في الحقل، ولتكن $x = \beta$ ، $y = \beta^3$ ، $z = \beta^5$.

عندئذ،

$$\begin{aligned} w^3 = x^3 + y^3 + z^3 &= \beta^3 + \beta^9 + \beta^{15} \\ &= 100 + 001 + 100 \\ &= \beta^4 \\ &= \beta^{18} \qquad (\text{لأن } \beta^7 = 1) \\ &= (\beta^6)^3 \end{aligned}$$

إذن، $w = \beta^6$. الآن، بوضع:

$$u = w + x + y + z = \beta^6 + \beta + \beta^4 + \beta^5 = \beta^4$$

وفرض أن $U = \{0, u\} = \{0, \beta^4\}$ وأن $V = \{w, x, y, z\} = \{\beta^6, \beta, \beta^3, \beta^5\}$ نجد أن $[\chi(U), \chi(V)] = 00001001\ 01010110$ كلمة شفرة تنتمي إلى $P(3)$ وزنها 6. ▲

تمرين

(**٩,٣,١٧**) إذا كان K^3 هو الحقل المنشأ باستخدام $1+\beta+\beta^3=0$ وإذا كانت $x,y,z\epsilon K^3$ هي العناصر المبيّنة في الفقرات التالية فعرِّف w و u كما في المبرهنة (**٩,٣,١٥**) لإنشاء كلمة شفرة وزنها 6 تنتمي إلى $P(3)$.

(أ) $x=\beta$ ، $y=\beta^2$ ، $z=\beta^3$.

(ب) $x=\beta$ ، $y=\beta^4$ ، $z=\beta^6$.

(ج) $x=\beta^0$ ، $y=\beta^3$ ، $z=\beta^6$.

مبرهنة (٩,٣,١٨)

$P(r)$ ليست شفرة خطيّة.

البرهان

لاحظنا في بداية هذا البند أن :

$$[\chi(U),\chi(V)]+[\chi(A),\chi(B)]=[\chi(U\Delta A),\chi(V\Delta B)]$$

وباستخدام المبرهنة (**٩,٣,١٥**) نستطيع انشاء كلمتي شفرة :

$$[\chi(U),\chi(V)],[\chi(A),\chi(B)]\epsilon P(r)$$

حيث $U=\{0,u_1\}$ ، $V=\{x_1,y_1,z_1,w_1\}$ ، $A=\{0,u_2\}$ ، $B=\{x_2,y_2,z_2,w_2\}$. عندئذ ، نرى استناداً إلى التمهيدية (**٩,٣,٥**) أن $c=[\chi(U\Delta A+u_1),\chi(V\Delta B)]$ كلمة شفرة تنتمي إلى $P(r)$. بما أن $|U\Delta A+u_1|\leq 2$ وبما أن المسافة بين c و $[\chi(U\Delta A+u_1),\chi(V\Delta B)]$ هي على الأكثر $2|U\Delta B+u_1|\leq 4$ وأن مسافة الشفرة $P(r)$ تساوي 6 نخلص إلى أن الكلمة $[\chi(U),\chi(V)]+[\chi(A),\chi(B)]$ ليست كلمة شفرة من كلمات $P(r)$. إذن ، $P(r)$ شفرة غير خطيّة. ■

الآن ، $P(r)$ غير خطيّة ، ولذا لا يوجد لها بُعد. كما أننا لا نعرف لحد الآن عدد كلمات الشفرة $P(r)$ ولكننا سنحصل على هذا العدد كنتيجة لعملية التشفير.

(٩,٤) تشفير شفرات بريبراتا الممتدة

Encoding Extended Preparata Codes

رأينا في البند (٥,٤) أن $g(x) = m_{\beta}(x)m_{\beta^3}(x)$ مولّد لشفرة BCH التي تُصوّب خطأين حيث مصفوفة اختبار النوعية هي:

$$H = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \\ \beta^{2^m-2} & \beta^{3(2^m-2)} \end{bmatrix} \qquad (٩,١)$$

وحيث β عنصر بدائي في الحقل $GF(2^r)$. تذكر أيضاً أن $deg(g(x)) = 2r$. وبما أن $g(x)$ كلمة شفرة غير صفرية وزنها أصغري فنرى عدم وجود تركيب خطي من أول $2r$ من صفوف المصفوفة (٩,١) بحيث يساوي صفراً. في الحقيقة، بما أن $g(x)$ تولّد شفرة دورية فإن أي مصفوفة جزئية مكوّنة من $2r$ من الصفوف المتتالية من المصفوفة H تكون صفوفها مُستقلة خطياً ومن ثم يوجد لها معكوس. لنفرض أن A هي المصفوفة الجزئية من H المكوّنة من الصفوف $2r$ الأخيرة (السفلى) ولنفرض أن H' هي المصفوفة الجزئية من H التي نحصل عليها بحذف الصفوف $2r$ الأخيرة.

مثال (٩,٤,١)

ليكن K^3 هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. عندئذ، يكون:

$$\begin{bmatrix} \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^6 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} \leftrightarrow A = \begin{bmatrix} 010 & 110 \\ 001 & 101 \\ 110 & 001 \\ 011 & 111 \\ 111 & 010 \\ 101 & 011 \end{bmatrix} \text{ و } A^{-1} = \begin{bmatrix} 001 & 011 \\ 111 & 010 \\ 011 & 101 \\ 110 & 100 \\ 101 & 110 \\ 111 & 001 \end{bmatrix}.$$

وإذا استخدمنا $x^5 + x^2 + 1$ لإنشاء K^5 (انظر المثال (**٥,١,١٥**)) نرى أن:

$$\begin{bmatrix} \beta^{21} & \beta^{63} \\ \beta^{22} & \beta^{66} \\ \vdots & \vdots \\ \beta^{30} & \beta^{90} \end{bmatrix} \leftrightarrow A = \begin{bmatrix} 00011 & 01000 \\ 10101 & 00001 \\ 11110 & 00101 \\ 01111 & 10001 \\ 10011 & 00111 \\ 11101 & 11011 \\ 11010 & 01100 \\ 01101 & 10101 \\ 10010 & 10011 \\ 01001 & 01101 \end{bmatrix} \text{ و } A^{-1} = \begin{bmatrix} 00111 & 00010 \\ 00011 & 10001 \\ 10011 & 00011 \\ 11011 & 01010 \\ 01101 & 10101 \\ 10101 & 11001 \\ 00110 & 11111 \\ 11001 & 01110 \\ 11000 & 00111 \\ 10001 & 10100 \end{bmatrix}. \qquad \blacktriangle$$

لنفرض أن $m = m_L, m_R$ أي كلمة ثنائية من الطول $2^{r+1} - 2r - 2$ حيث m_L كلمة ثنائية طولها $2^r - 1$ و m_R كلمة ثنائية طولها $2^r - 2r - 1$. عندئذ، بتمثيل m_L و m_R باستخدام كثيرات الحدود نرى أن:

$$[m_L(\beta), m_L(\beta^3)] \leftrightarrow m_L H$$
$$[m_R(\beta), m_R(\beta^3)] \leftrightarrow m_R H$$

نعرّف الآن:

$$v_R = [m_L(\beta) + m_R(\beta), m_L(\beta^3) + \left(m_L(\beta)\right)^3 + m_R(\beta^3)]A^{-1}.$$

مبرهنة (٩,٤,٢)

لنفرض أن r عدد فردي ولنفرض أن m أي كلمة ثنائية من الطول $2^{r+1} - 2r - 2$. إذا كان $\chi(U) = [m_L, p_L]$ و $\chi(V) = [m_R, v_R, p_R]$ حيث p_L و p_R إحداثي اختبار نوعية لكل من m_L و $[m_R, v_R]$ على التوالي فإن $[\chi(U), \chi(V)] \epsilon P(r)$.

البرهان

$$\begin{aligned} [m_R, v_R]H &= [m_R]H' + [v_R]A \\ &= [m_R(\beta), m_R(\beta^3)] + [m_L(\beta) + m_R(\beta), m_L(\beta^3) + \left(m_L(\beta)\right)^3 + m_R(\beta^3)] \\ &= [m_L(\beta), m_L(\beta^3) + \left(m_L(\beta)\right)^3]. \end{aligned}$$

ولكن $[m_R, v_R]H = [\sum_{v\epsilon V} v, \sum_{v\epsilon V} v^3]$. وبالمثل، نرى أن $m_L(\beta) = \sum_{u\epsilon U} u$ وأن:

$$m_L(\beta^3) + \left(m_L(\beta)\right)^3 = \sum_{u\epsilon U} u^3 + \left(\sum_{u\epsilon U} u\right)^3$$

وبهذا يتحقق الشرطان (ii) و (iii) من التعريف (**٩,٣,٣**). ومن الواضح أن الشرطين (i) و (iv) محققان. إذن، $[\chi(U),\chi(V)]\epsilon P(r)$. ■

نتيجة (٩,٤,٣)

عدد كلمات الشفرة $P(r)$ يساوي $2^{2^{r+1}-2r-2}$.

البرهان

استناداً إلى المبرهنة (**٩,٤,٢**)، يوجد عدد $2^{2^{r+1}-2r-2}$ خياراً للكلمة m وكل منها يؤدي إلى كلمة شفرة مختلفة. بقية إحداثيات كلمة الشفرة التي تحتوي m تتحدد تماماً بالشروط (i) ، (ii) ، (iii) من التعريف (**٩,٣,٣**). ■

خوارزمية (٩,٤,٤) [تشفير $P(r)$]

لتكن m_L و m_R كلمتين من الطول 2^{r-1} و 2^r-r-1 على التوالي. ولتكن v_R معرفة كما في المبرهنة (**٩,٤,٢**). عندئذ، $[m_L,p_L,m_R,v_R,p_R]$ كلمة شفرة تقابل الرسالة $m=[m_L,m_R]$.

مثال (٩,٤,٥)

لنفرض أن $r=3$ ، $m_L=0110010$ ، $m_R=1$. عندئذ،

$$m_L(\beta)=\beta+\beta^2+\beta^5=\beta^0, m_R(\beta)=\beta^0$$
$$m_L(\beta^3)=\beta^0\ ,m_L(\beta^3)=\beta^3+\beta^6+\beta^{15}=\beta^2$$
$$v_R=[\beta^0+\beta^0,\beta^2+\beta^2+\beta^0+\beta^0]A^{-1}$$
$$=[000,001]A^{-1}=111001$$

حيث A^{-1} هي المصفوفة المقدمة في المثال (**٩,٤,١**). إذن، تُشفّر الرسالة $m=[0110010\ ,1]$ إلى كلمة الشفرة $c=[m_L,p_L,m_R,v_R,p_R]=[0110010\ ,1\ ,1\ ,111001\ ,1]$. وباستخدام ترميز البند (**٩,١**) تكون $c=[\chi(U),\chi(V)]$ حيث $\chi(U)=01100101$ و $\chi(V)=11110011$. هذه هي كلمة الشفرة من $P(3)$ المبيّنة في المثال (**٩,٣,٤**). ▲

تمارين

(**٩,٤,٦**) إذا كان K^3 هو الحقل المنشأ باستخدام $x^3 + x + 1$ وكانت A^{-1} هي المصفوفة المبيّنة في المثال (**٩,٤,١**) فاستخدم $P(3)$ لتشفير كل من الرسائل التالية :

(أ) $m_L = 1010100$ و $m_R = 1$.

(ب) $m_L = 1010100$ و $m_R = 0$.

(ج) $m_L = 1111111$ و $m_R = 1$.

(د) $m_L = 1111111$ و $m_R = 0$.

(هـ) $m_L = 0000000$ و $m_R = 1$.

(**٩,٤,٧**) إذا كان K^5 هو الحقل المنشأ باستخدام $x^5 + x^2 + 1$ وكانت A^{-1} هي المصفوفة المبيّنة في المثال (**٩,٤,١**) فاستخدم $P(5)$ لتشفير كل من الرسائل التالية :

(أ) $m_L = 10100 \cdots 0$ و $m_R = 000001000100 \cdots 0$.

(ب) $m_L = 10100 \cdots 0$ و $m_R = 00 \cdots 0$.

(ج) $m_L = 10100 \cdots 0$ و $m_R = 11110 \cdots 0$.

(د) $m_L = 00 \cdots 0$ و $m_R = 100 \cdots 0$.

(**٩,٤,٨**) جد طول كل من (أ) m_L و (ب) m_R المعطاة في التمرين (**٩,٤,٧**).

(٩,٥) فك تشفير شفرات بريبراتا الممتدة
Decoding Extended Preparata Codes

وجدنا أن مسافة الشفرة $P(r)$ تساوي 6 (مبرهنة (**٩,٣,١٥**))، وبهذا نحتاج إلى خوارزمية تُصوّب خطأين على الأكثر. لنفرض أن w هي الكلمة المستقبلة ولنفرض أن $w = [m_L, p_L, w_R, p_R]$ حيث كل من w_L و w_R كلمة من الطول $2^r - 1$ وأن كلاً من p_L و p_R إحداثي اختبار النوعية. عندئذ، نقوم بحساب $[w_L(\beta), w_L(\beta^3)] = w_L H$ و $[w_R(\beta), w_R(\beta^3)] = w_R H$.

ندرس الحالات التالية اعتماداً على أماكن وقوع الأخطاء:

(١) إذا اقتصر وقوع الأخطاء على إحداثيي اختبار النوعية فنرى استناداً إلى الشرطين (ii) و (iii) من التعريف (**٩,٣,٣**) أن:

$$w_L(\beta) = w_R(\beta)$$

$$.w_L(\beta^3) + \left(w_L(\beta)\right)^3 = w_R(\beta^3)$$

(٢) إذا كانت w_L خالية من الأخطاء ووجد خطأ واحد في الموقع i من w_R وعلى الأكثر خطأ واحد في إحداثيي اختبار النوعية فنرى أن:

$$w_L(\beta) = w_R(\beta) + \beta^i$$

$$w_L(\beta^3) + \left(w_L(\beta)\right)^3 = w_R(\beta^3) + \beta^{3i}$$

إذن، $\left(w_L(\beta) + w_R(\beta)\right)^3 = w_L(\beta^3) + \left(w_L(\beta)\right)^3 + w_R(\beta^3)$

(استناداً إلى الشرطين (ii) و (iii) من التعريف (**٩,٣,٣**)). إذا تحققت المساواة الأخيرة فنكتب $\beta^i = w_L(\beta) + w_R(\beta)$ ونقوم بتغيير الإحداثي i من w_R وعلى الأكثر إحداثي اختبار نوعية واحد.

(٣) إذا كانت w_R خالية من الأخطاء ووجد خطأ واحد في الموقع i من w_L وعلى الأكثر خطأ واحد في مرتبتي اختبار النوعية فنرى اعتماداً على الفقرة (i) من التمهيدية (**٩,٣,٨**) أن بإمكاننا تكرار الخطوة (٢) لنجد:

$$.\left(w_R(\beta) + w_L(\beta)\right)^3 = \left(w_R(\beta^3) + w_R(\beta)\right)^3 + w_L(\beta^3)$$

وفي هذه الحالة نضع $\beta^i = w_R(\beta) + w_L(\beta)$ ونقوم بتغيير الإحداثي i من w_L وعلى الأكثر إحداثي اختبار نوعية واحد.

(٤) إذا وقع خطآن في w_R، في الموقعين i و j فنجد باستخدام التعريف (**٩,٣,٣**) أن:

$$w_L(\beta) = w_R(\beta) + \beta^i + \beta^j$$

$$.w_L(\beta^3) + \left(w_L(\beta)\right)^3 = w_R(\beta^3) + \beta^{3i} + \beta^{3j}$$

وبهذا نستطيع معرفة $\beta^i + \beta^j$ و $\beta^{3i} + \beta^{3j}$. أما i و j فنستطيع ايجادهما الآن بالاسلوب المستخدم في الشفرة BCH التي تُصوّب أنماط أخطاء من النوع 2 (انظر البند (**٥,٥**)).

(٥) إذا وقع خطآن في w_L فمن الممكن استخدام التمهيدية (**٩,٣,٨**) (i) (كما في الحالة (٣)) ونقاش الخطوة (٤) لإيجاد مواقع الخطأين.

(٦) إذا وقع خطأ في w_L وخطأ في w_R في الموقعين i و j على التوالي فنجد استناداً إلى التعريف (**٩,٣,٣**) أن:

$$w_L(\beta) + \beta^i = w_R(\beta) + \beta^j$$

$$w_L(\beta^3) + \beta^{3i} + (w_L(\beta) + \beta^i)^3 = w_R(\beta^3) + \beta^{3j}$$

وبحل هاتين المعادلتين لإيجاد β^i و β^j نجد من المعادلة الأولى:

$$\beta^j = w_L(\beta) + \beta^i + w_R(\beta)$$

وبالتعويض في المعادلة الثانية نرى أن:

$$\begin{aligned} w_L(\beta^3) &+ \beta^{3i} + (w_L(\beta) + \beta^i)^3 \\ &= w_R(\beta^3) + (w_L(\beta) + \beta^i)^3 + (w_L(\beta) + \beta^i)^2 w_R(\beta) \\ &+ (w_L(\beta) + \beta^i) w_R(\beta)^2 + w_R(\beta)^3 \end{aligned}$$

بالتبسيط نحصل على:

$$\begin{aligned} \beta^{3i} &+ \beta^{2i} w_R(\beta) + \beta^i \big(w_R(\beta)\big)^2 + \big(w_R(\beta)\big)^3 \\ &= w_L(\beta^3) + w_R(\beta^3) + w_L(\beta)^2 w_R(\beta) + w_L(\beta) w_R(\beta)^2 \end{aligned}$$

وبهذا نرى أن:

$$\begin{aligned} \big(\beta^i + w_R(\beta)\big)^3 &= \big(w_L(\beta^3) + w_R(\beta^3)\big) + \big(w_L(\beta) + w_R(\beta)\big)^3 + w_L(\beta)^3 + w_R(\beta)^3 \\ &= \Delta \end{aligned}$$

إذن:

$$\beta^i = w_R(\beta) + \Delta^{1/3}$$

$$.\beta^j = w_L(\beta) + \Delta^{1/3}$$

وبهذا نرى أن بالإمكان ايجاد جميع مواقع الأخطاء. تُسهّل علينا شروط اختبار النوعية على كل من نصفي w في اختيار الحالة التي تطبق على w. وبهذا نحصل على خوارزمية فك التشفير التالية حيث خطواتها تقابل الحالات التي درسناها في هذا البند.

خوارزمية (٩,٥,١) [فك تشفير $P(r)$]

لتكن $w = [m_L, p_L, w_R, p_R]$ كلمة مستقبلة.

(٠) احسب $L_1 = w_L(\beta)$ ، $L_3 = w_L(\beta^3)$ ، $R_1 = w_R(\beta)$ ، $R_3 = w_R(\beta^3)$.

(١) إذا كان $L_1 + R_1 = 0$ و $L_3 + L_1^3 + R_3 = 0$ فتقع الأخطاء فقط في إحداثيي اختبار النوعية.

(٢) إذا كان $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = 0$ فضع $\beta^i = L_1 + R_1$. صوّب الموقع i من w_R وإحداثي اختبار نوعية واحدة على الأكثر. اطلب إعادة ارسال إذا احتجت إلى تغيير إحداثيي اختبار النوعية.

(٣) إذا كان $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = 0$ فضع $\beta^i = L_1 + R_1$. صوّب الموقع i من w_L وإحداثي اختبار نوعية واحد على الأكثر. اطلب إعادة ارسال إذا احتجت إلى تغيير إحداثيي اختبار النوعية.

(٤) إذا كانت نوعية كل من نصفي w زوجية ووجد i و j بحيث يكون:

$$x^2 + (L_1 + R_1)x + \frac{L_3 + L_1^3 + R_3 + (L_1 + R_1)^3}{L_1 + R_1} = (x + \beta^i)(x + \beta^j)$$

فصوّب الموقعين i و j من w_L.

(٥) إذا كانت نوعية كل من نصفي w زوجية ووجد i و j بحيث يكون:

$$x^2 + (L_1 + R_1)x + \frac{R_3 + R_1^3 + L_3 + (L_1 + R_1)^3}{L_1 + R_1} = (x + \beta^i)(x + \beta^j)$$

فصوّب الموقعين i و j من w_R.

(٦) إذا كانت نوعية كل من نصفي w فردية فضع :

$$\beta^i = R_1 + (L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3)^{1/3}$$

$$.\beta^j = L_1 + (L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3)^{1/3}$$

صوّب الموقع i من w_L والموقع j من w_R.

(٧) إذا لم تحصل على كلمة شفرة هي الأقرب فاستنتج وقوع على الأقل ثلاثة أخطاء أثناء الإرسال واطلب إعادة إرسال.

مثال (٩,٥,٢)

فك تشفير كل من الكلمات المستقبلة التالية إذا علمت أنها شُفّرت باستخدام الشفرة $P(3)$، علماً بأنه قد تم إنشاء الحقل $GF(2^3)$ باستخدام $1 + x + x^3$.

(أ) 11100111 10010011.

(ب) 10001001 10100100.

(ج) 11101001 10001000.

الحل

فك تشفير (أ):

(٠) $[L_1, L_3] = w_L H = [111,110]$ و $[R_1, R_3] = w_R H = [101,110]$.

(١) $L_1 + R_1 = 111 + 101 = \beta \neq 0$.

(٢) $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^3 + \beta^3 + \beta^{15} + \beta^3 = \beta^0 \neq 0$.

(٣) $(L_1 + R_1)^3 + R_3 + R_1^3 + L_1 = \beta^3 + \beta^3 + \beta^{18} + \beta^3 = \beta^6 \neq 0$.

(٤) $x^2 + \beta x + \frac{\beta^3+\beta^{15}+\beta^3+\beta^3+\beta^3}{\beta} = x^2 + \beta x + \beta^6 = (x + \beta^2)(x + \beta^4)$

فك تشفير w إلى 11001111 10010011.

فك تشفير (ب):

(٠) $[L_1, L_3] = w_L H = [010,011]$ و $[R_1, R_3] = w_R H = [111,011]$.

(١) $L_1 + R_1 = 010 + 111 = \beta^6 \neq 0$.

(٢) $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^{18} + \beta^4 + \beta^3 + \beta^4 = \beta^6 \neq 0$.

(٣) $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = \beta^{18} + \beta^4 + \beta^{15} + \beta^4 = \beta^2 \neq 0$.

(٤) و (٥) نوعية كل من نصفي w فردية.

(٦)
$$\begin{aligned} \beta^i &= \beta^5 + (\beta^3 + \beta^{15} + \beta^{18} + \beta^4 + \beta^4)^{1/3} \\ &= \beta^5 + (\beta^5)^{1/3} \\ &= \beta^5 + (\beta^{12})^{1/3} \\ &= \beta^5 + \beta^4 \\ &= \beta^0 \end{aligned}$$

إذن، $i = 0$ ونضع مباشرة:

$\beta^j = \beta + \beta^4 = \beta^2$.

إذن، $j = 2$ ويكون فك تشفير w هو 10101001 00100100.

فك تشفير (ج):

(٠) $[L_1, L_3] = w_L H = [111{,}011]$ و $[R_1, R_3] = w_R H = [100{,}000]$.

(١) $L_1 + R_1 = 11 + 100 = \beta^4 \neq 0$.

(٢) $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^{12} + \beta^4 + \beta^{15} + 0 = \beta^3 \neq 0$.

(٣) $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = \beta^{12} + 0 + \beta^0 + \beta^4 = \beta^2 = 0$.

ضع $\beta^i = L_1 + R_1 = \beta^4$. ولذا $i = 4$. ولكن تغيير الموقع 4 من w_L يتطلب تغيير إحداثيي اختبار النوعية. وبهذا نطلب اعادة ارسال لأننا نستطيع إيجاد كلمة شفرة تبعد مسافة 3 عن الكلمة w. ▲

تمارين

(٩,٥,٣) فك تشفير كل من الكلمات المستقبلة التالية التي تم تشفيرها باستخدام $P(3)$ علماً بأنه استخدمت $1 + x + x^3$ لانشاء $GF(2^3)$.

(أ) 10000001 , 11101000 (ب) 00011010 , 01000010

(ج) 00100101 , 10100100 (د) 01010110 , 00011110

(هـ) 11101000 , 10001001 (و) 10011001 , 01010101

(ز) 01000111 , 11001000 (ح) 10101101 , 11010000

(ط) 11101110 , 01010101 (ي) 10111011 , 01101010

(ك) 01011101 , 11101101 (ل) 10011100 , 10100100

(م) 01101101 , 10011000 (ن) 10101010 , 10111011

(س) 10100101 , 00010001

(**٩,٥,٤**) فك تشفير كل من الكلمات المستقبلة التالية التي تم تشفيرها باستخدام $P(5)$ علماً بأنه استخدمت $1 + x^2 + x^5$ لإنشاء الحقل $GF(2^5)$ (انظر التمرين (**٥,١,١٥**)).

(أ) 11000 11000 10000 00000 00000 10000 10 ,
00011 11000 00000 00000 00011 00100 00

(ب) 10100 00000 10000 00000 00000 00000 00 ,
00000 10001 00000 00100 01010 10111 00

(**٩,٥,٥**) لنفرض أن w هي كلمة مستقبلة بحيث إن نوعية نصفها الأيسر فردية ونوعية نصفها الأيمن زوجية. هل من الممكن استخدام الخطوة (٢) من الخوارزمية (**٩,٥,١**) لفك تشفير w إلى كلمة شفرة تبعد مسافة 2 عن w ؟